

# Access Point

---

AT-WL2411



## Installation and User's Guide



PN 613-50229-00 Rev B

Simply connecting the  world

Copyright © 2002 Allied Telesyn, Inc.  
960 Stewart Drive Suite B, Sunnyvale, CA 94085 USA

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesyn, Inc.

Microsoft is a registered trademark of Microsoft Corporation, Netscape Navigator is a registered trademark of Netscape Communications Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesyn, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesyn, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesyn, Inc. has been advised of, known, or should have known, the possibility of such damages.

# Electrical Safety and Emission Statement

**Standards:** This product meets the following standards.

## U.S. Federal Communications Commission

### Declaration Of Conformity

Manufacture Name: Allied Telesyn, Inc.  
Manufacture Address: 960 Stewart Drive, Suite B  
Sunnyvale, CA 94085 USA  
Manufacture Telephone: 408-730-0950  
Declares that the product: Access Point  
Model Numbers: AT-WL2411

This product complies with FCC Part 15B, Class B Limits:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device must not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

### Radiated Energy

Note: This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with instructions, may cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on. The user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Changes and modifications not expressly approved by the manufacturer or registrant of this equipment can void your authority to operate this equipment under Federal Communications Commission rules.

## Canadian Department of Communications


This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.


RFI Emission


EN55022 Class B  1


Immunity


EN55024  2


Electrical Safety


EN60950 (TUV), UL1950 (UL/cUL)  3


**Important:** Appendix C contains translated safety statements for installing this equipment. When you see the , go to Appendix C for the translated safety statement in your language.


**Wichtig:** Anhang C enthält übersetzte Sicherheitshinweise für die Installation dieses Geräts. Wenn Sie  sehen, schlagen Sie in Anhang C den übersetzten Sicherheitshinweis in Ihrer Sprache nach.


**Vigtigt:** Tillæg C indeholder oversatte sikkerhedsadvarsler, der vedrører installation af dette udstyr. Når De ser symbolet , skal De slå op i tillæg C og finde de oversatte sikkerhedsadvarsler i Deres eget sprog.


**Belangrijk:** Appendix C bevat vertaalde veiligheidsopmerkingen voor het installeren van deze apparatuur. Wanneer u de  ziet, raadpleeg Appendix C voor vertaalde veiligheidsinstructies in uw taal.


**Important:** L'annexe C contient les instructions de sécurité relatives à l'installation de cet équipement. Lorsque vous voyez le symbole , reportez-vous à l'annexe C pour consulter la traduction de ces instructions dans votre langue.


**Tärkeää:** Liite C sisältää tämän laitteen asentamiseen liittyvät käännettyt turvaohjeet. Kun näet -symbolin, katso käännettyä turvaohjetta liitteestä C.

**Importante:** L'Appendice C contiene avvisi di sicurezza tradotti per l'installazione di questa apparecchiatura. Il simbolo , indica di consultare l'Appendice C per l'avviso di sicurezza nella propria lingua.

**Viktig:** Tillegg C inneholder oversatt sikkerhetsinformasjon for installering av dette utstyret. Når du ser , åpner du til Tillegg C for å finne den oversatte sikkerhetsinformasjonen på ønsket språk.

**Importante:** O Anexo C contém advertências de segurança traduzidas para instalar este equipamento. Quando vir o símbolo , leia a advertência de segurança traduzida no seu idioma no Anexo C.

**Importante:** El Apéndice C contiene mensajes de seguridad traducidos para la instalación de este equipo. Cuando vea el símbolo , vaya al Apéndice C para ver el mensaje de seguridad traducido a su idioma.

**Obs!** Bilaga C innehåller översatta säkerhetsmeddelanden avseende installationen av denna utrustning. När du ser , skall du gå till Bilaga C för att läsa det översatta säkerhetsmeddelandet på ditt språk.

# Table of Contents

---

<b>Preface</b> .....	11
How This Guide is Organized .....	11
Document Conventions .....	13
Where to Find Web-based Guides .....	14
Contacting Allied Telesyn Technical Support .....	15
Online Support.....	15
Telephone Support.....	15
E-mail Support .....	15
Returning Products .....	16
For Sales or Corporate Information .....	17
Management Software Updates .....	18
 <b>Chapter 1</b>	
<b>Product Description</b> .....	19
Summary of Features .....	19
Hardware Features .....	20
Status LEDs .....	20
Ports .....	21
10 Mbps Twisted Pair Ethernet Port .....	21
Serial Port .....	22
Serial Cable .....	22
Power Supply Input Port.....	22
External AC/DC Power Adapter.....	22
Firmware Features .....	23
Network Configurations .....	24
A Simple Wireless Network.....	24
Using Multiple APs and Roaming End Devices.....	25
Using APs to Create a Point-to Point Bridge.....	26
 <b>Chapter 2</b>	
<b>Installation</b> .....	27
Installation Safety Precautions .....	28
Selecting a Site for the Access Point .....	29
Cables Not Included .....	31
Unpacking the Access Point .....	32
Installing the Access Point .....	33
Mounting.....	33
Positioning the Antenna.....	34

Cabling.....	34
Powering On.....	35
Attaching an External Antenna (Optional) .....	36
Warranty Registration .....	38
<b>Chapter 3</b>	
<b>Configuration Overview .....</b>	<b>39</b>
Using a Serial Connection .....	39
Assigning an IP Address .....	42
Using a Web Browser .....	44
Saving Your Configuration Changes .....	46
Using a Telnet Session .....	47
Using SNMP .....	48
Configuring the SNMP Community .....	48
<b>Chapter 4</b>	
<b>Configuring the Ethernet Network .....</b>	<b>50</b>
Configuring the TCP/IP Settings .....	50
Configuring the Access Point as a DHCP Client.....	52
Configuring the Access Point as a DHCP Server.....	53
About Network Address Translation (NAT).....	56
Configuring the Access Point as an ARP Server.....	58
Configuring the Access Point to Send ARP Requests.....	60
Configuring the Ethernet Settings .....	62
Configuring Ethernet Filters .....	64
Configuring the Ethernet Address Table.....	64
Using Ethernet Frame Type Filters .....	65
Configuring Advanced Filters .....	71
<b>Chapter 5</b>	
<b>Configuring the Spanning Tree .....</b>	<b>74</b>
Configuring the Spanning Tree Parameters .....	74
About the Root Access Point .....	77
About Bridging .....	78
Bridging Layer Functions .....	79
About Secondary LANs and Designated Bridges.....	80
Configuring Global Parameters .....	82
Configuring Global Flooding.....	82
Configuring Global RF Parameters .....	85
About IP Tunnels .....	88
Internet Group Management Protocol (IGMP) .....	89
Originating IP Tunnels .....	90
Establishing and Maintaining IP Tunnels .....	91
IP Addressing for End Devices .....	92
Using Non-IP Protocols.....	92
Frame Forwarding .....	92
Configuring IP Tunnels .....	94
Configuring IP Tunnel Filters .....	98
Using IP Tunnel Frame Type Filters .....	98
<b>Chapter 6</b>	
<b>Configuring the Radio .....</b>	<b>105</b>
About the Radios .....	105
Configuring the IEEE 802.11b Radio .....	106
Worldwide Frequencies for the 802.11b Radio.....	108
Configuring 802.11b Radio Advanced Parameters .....	109

Configuring a Voice Network.....	112
Configuring WAPs .....	115
Configuring Point-to-Point Bridges .....	118
<b>Chapter 7</b>	
<b>Configuring Security</b> .....	124
About Security .....	124
Enabling Access Methods .....	125
Setting Up Logins .....	127
Configuring the Internal RADIUS Server .....	130
Using 802.1x Security .....	132
<b>Chapter 8</b>	
<b>Access Point Maintenance</b> .....	136
Monitoring the Access Point .....	136
Viewing Access Point Connections.....	136
Viewing Port Statistics .....	137
Viewing the Configuration Summary .....	138
Viewing Information About the Access Point.....	139
Restoring the Default Settings .....	140
Upgrading the Firmware .....	141
Using a Serial Connection .....	141
Using TFTP via Telnet.....	143
Using a Web Browser .....	144
<b>Chapter 9</b>	
<b>Troubleshooting</b> .....	146
LEDs .....	146
Radio .....	148
LEDs.....	148
Communications Program or Telnet.....	148
Radio MAC Ping .....	148
ICMP Echo .....	149
Problems During Web Browser Firmware Upgrade .....	150
Commonly Asked Technical Support Questions .....	151
Getting Help with Your Installation .....	154
<b>Chapter 10</b>	
<b>Advanced Configuration Commands</b> .....	155
Using the Access Point Monitor .....	155
Understanding Access Point Segments.....	155
Entering the Access Point Monitor .....	156
Using Access Point Monitor Commands .....	157
B.....	157
FX.....	158
FD .....	158
FR.....	158
MR .....	158
SR.....	158
Using Service Mode Commands .....	160
SRVC .....	160
FFR .....	161
PN .....	161
PQ.....	161
Using Test Mode Commands .....	162
TEST .....	162

Using Console Command Mode .....	164
Using Console Commands .....	165
fb .....	165
fd .....	166
fdel .....	166
fe .....	167
script .....	167
Using Sdvars Commands .....	168
sdvars set serveripaddress.....	168
sdvars set scriptfilename.....	168
sdvars set starttime .....	169
sdvars set checkpoint.....	169
sdvars set terminate .....	170
sdvars set setactivepointers.....	170
sdvars set nextpoweruptime.....	171
Using TFTP Commands .....	172
tftp get.....	172
tftp put.....	174
tftp server log .....	175
tftp server start .....	175
tftp server stop .....	175

## Appendix A

<b>Default Configuration Settings</b> .....	178
TCP/IP Menu Default Settings .....	178
IEEE 802.11b Radio Menu Default Settings .....	179
Wireless Bridging .....	179
Advanced Configuration .....	179
Spanning Tree Settings Menu Default Settings .....	180
Global Flooding.....	180
Global RF Parameters .....	181
Ethernet Menu Default Settings .....	182
Address Table.....	182
Frame Type Filters .....	182
Predefined Subtype Filers .....	183
Customizable Subtype Filters .....	183
Advanced Filters.....	183
IP Tunnels Menu Default Settings .....	184
Tunnel Filters .....	184
Network Management Menu Default Settings .....	185
Community Strings .....	185
Security Menu Default Settings .....	186
Passwords .....	186
802.1x .....	186
IEEE 802.11b Radio WEP .....	186
Internal RADIUS Server .....	186

## Appendix B

<b>Technical Specifications</b> .....	187
Physical Specifications .....	187
Environmental Specifications .....	187
Power Specifications .....	187
Safety and Electromagnetic Emissions Certifications .....	187
Standards .....	187
Other Specifications .....	188
IEEE 802.11b Radio Specifications .....	188



**Appendix C**

<b>Translated Electrical Safety and Emission Information .....</b>	<b>189</b>
<b>Glossary .....</b>	<b>202</b>



# Preface

---

This guide contains instructions on how to install and configure the AT-WL2411 access point.

## How This Guide is Organized

---

This manual contains the following chapters and appendices:

**Chapter 1, Product Description**, describes the features and components of the access point.

**Chapter 2, Installation**, contains installation and mounting instructions.

**Chapter 3, Configuration Overview**, explains how to access the configuration firmware.

**Chapter 4, Configuring the Ethernet Network**, explains how to configure the Ethernet settings on the access point.

**Chapter 5, Configuring Spanning Tree**, explains how to configure the Spanning Tree settings on the access point.

**Chapter 6, Configuring the Radios**, explains how to configure the radio settings on the access point.

**Chapter 7, Configuring Security**, explains how to configure the security settings for the access point.

**Chapter 8, Maintenance**, provides information on how to monitor the performance of the access point and upgrade the firmware.

**Chapter 9, Troubleshooting**, explains how to identify and resolve common problems that occur with the access point.

**Chapter 10, Advanced Configuration Commands,** contains commands for advanced access point users.

**Appendix A, Default Settings,** lists the default firmware settings.

**Appendix B, Technical Specifications,** lists the technical specifications for the access point.

**Appendix C, Translated Electrical Safety and Emission Information,** contains multi-language translations of the warnings and cautions in the manual.

**Glossary,** contains definitions for technical terms that you may not be familiar with.

## Document Conventions

---

This document uses the following conventions:

---

**Note**

Notes provide additional information.

---

**Warning**

Warnings inform you that performing or omitting a specific action may result in bodily injury.

---

**Caution**

Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

---

## Where to Find Web-based Guides

---

The Allied Telesyn Web site at [www.alliedtelesyn.com](http://www.alliedtelesyn.com) offers you an easy way to access the most recent documentation, software, and technical information for all Allied Telesyn products. For product guides, select the [Support and Services](#) link. The documents can be viewed online or downloaded onto a local workstation or server.

## Contacting Allied Telesyn Technical Support

---

You can contact Allied Telesyn technical support online or by telephone or e-mail.

### Online Support

You can request technical support online by accessing the Knowledge Base at <http://kb.alliedtelesyn.com>. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

### Telephone Support

For technical support by telephone, contact Allied Telesyn at one of the following locations:

#### Americas

United States, Canada, Mexico, Central America, South America  
Tel: 1 (800) 428-4835

#### Asia

Singapore, Taiwan, Thailand, Malaysia, Indonesia, Korea, Philippines, China, India, Hong Kong  
Tel: (+65) 3815-612

#### Australia

Tel: 1 (800) 000-880

#### France

France, Belgium, Luxembourg, The Netherlands, Middle East, Africa  
Tel: (+33) 0-1-60-92-15-25

#### Germany

Germany, Switzerland, Austria, Eastern Europe  
Tel: (+49) 30-435-900-126

#### Italy

Italy, Spain, Portugal, Greece, Turkey, Israel  
Tel: (+39) 02-41-30-41

#### Japan

Tel: (+81) 3-3443-5640

#### United Kingdom

United Kingdom, Denmark, Norway, Sweden, Finland  
Tel: (+0044) 1235-442500

### E-mail Support

To contact Allied Telesyn via e-mail for technical support, use the e-mail address appropriate to your region:

#### Latin America, Mexico, Puerto Rico, Caribbean, and Virgin Islands

[latin\\_america@alliedtelesyn.com](mailto:latin_america@alliedtelesyn.com)

#### Europe

[support\\_europe@alliedtelesyn.com](mailto:support_europe@alliedtelesyn.com)

## Returning Products

---

Products for return or repair must first be assigned a Return Materials Authorization (RMA) number. A product sent to Allied Telesyn without a RMA number will be returned to the sender at the sender's expense.

To obtain an RMA number, contact Allied Telesyn's Technical Support at one of the following locations:

**North America**

Toll-free: 1-800-762-1664

Fax: 1-425-806-1050

**Europe, Africa, and the Middle East**

Tel: +44-1793-501401

Fax: +44-1793-431099

**Latin America, the Caribbean, and Virgin Islands**

Tel: international code + 425-481-3852 1-800-424-5012, ext 3852 or 1-800-424-4284, ext 3852

Fax: international code + 425-481-3895

**Puerto Rico**

Tel: 1-800-424-5012, ext 3852 or

1-800-424-4284, ext 3852

**Mexico**

Toll-free: 800-424-5012, ext 3852

Fax: international code + 425-481-3895

**Asia and Southeast Asia**

Tel: +65-381-5612

Fax: +65-383-3830

**Australia**

Toll-free: 1-800-000-880

Fax: +61-2-9438-4966

**New Zealand**

Toll-free: 0800-45-5782



## For Sales or Corporate Information

---

You can contact Allied Telesyn for sales or corporate information at:

**Allied Telesyn, Inc.**

19800 North Creek Parkway,

Suite 200

Bothell, WA 98011

Tel:1 (425) 487-8880

Fax:1 (425) 489-9191

## Management Software Updates

---

Allied Telesyn periodically updates the firmware programs for our managed products. You can download new versions of our firmware from our Web site at [www.alliedtelesyn.com](http://www.alliedtelesyn.com) or from our FTP server at [ftp.alliedtelesyn.com](ftp://ftp.alliedtelesyn.com). To use the FTP server, enter "anonymous" for the user name and use your e-mail address for the password.

## Chapter 1

# Product Description

---

The AT-WL2411 access point forwards data from wireless end devices to the wired Ethernet network. The AT-WL2411 can be used as an access point or as a point-to-point bridge. An access point is connected to a wired network and provides network access for wireless end devices. A point-to-point bridge connects two wired LANs and is often used to provide wireless communications in locations where running cable is difficult, such as across roads or between buildings. The AT-WL2411 accommodates one 802.11b radio. The AT-WL2411 is ideal for use in networks that do not need mixed radios or when configured as a station at the remote end of a wireless hop to a secondary LAN.

## Summary of Features

---

- ☐ Supports IEEE 802.11b radios
- ☐ Installed 802.11b radio is Wi-Fi certified
- ☐ 10 Mbps Ethernet port with an RJ-45 connector
- ☐ Status LEDs
- ☐ Serial port for initial configuration and management
- ☐ Version 1.72 configuration firmware
- ☐ 5 V DC external power supply input port
- ☐ Configuration via serial connection, Web browser, Telnet, and SNMP
- ☐ Can be used a DHCP server or client
- ☐ Can support 256 wireless end devices

## Hardware Features

---

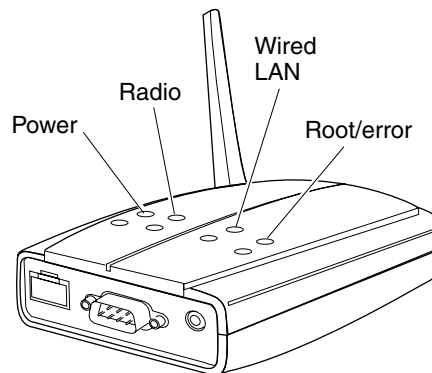
The following sections describe these hardware features of the AT-WL2411 access point:

- ☐ Status LEDs
- ☐ 10 Mbps twisted pair Ethernet port
- ☐ Serial connection management port
- ☐ Serial connection management cable
- ☐ 5V DC power supply input port
- ☐ External AC/DC power adapter

**Status LEDs**    The AT-WL2411 features the following status LEDs:

- ☐ Power
- ☐ Radio
- ☐ Wired LAN: Ethernet link and activity
- ☐ Root/error

Figure 1 illustrates the four LEDs on the AT-WL2411.



**Figure 1** System LEDs

Table 1 defines the LEDs for the AT-WL2411 access point.

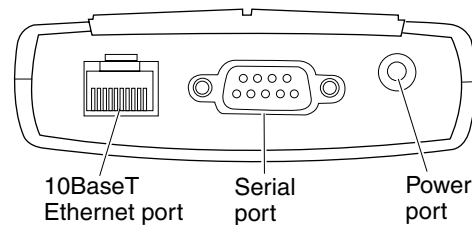
**Table 1** Status LEDs

LED	Color	Description
PWR	Green	Power is applied to the unit.
Radio	Green	Flashes when a frame is transmitted or received on the radio port.
Wired LAN	Green	Flashes when a frame is transmitted or received on the Ethernet port.
Root/error	Green	Flashes if access point has been configured as root; remains on if an error is detected.

**Ports** The AT-WL2411 features the following ports:

- ☐ Ethernet
- ☐ Serial connection/management
- ☐ Power

Figure 2 illustrates the ports on the AT-WL2411.



**Figure 2** System Ports

### 10 Mbps Twisted Pair Ethernet Port

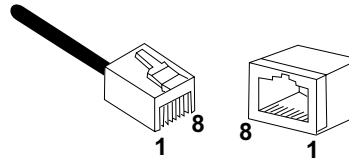
The AT-WL2411 access point has one twisted pair Ethernet port. The twisted pair port features an RJ-45 connector with a maximum operating distance of 100 meters (328 feet). The Ethernet port is used to connect the access point to your Ethernet network.

### Type of Cabling

The 10Base-T twisted pair port on the AT-WL2411 access point is designed to operate with a Category 3 or better 100 ohm unshielded twisted pair cable.

## RJ-45 Port Pinouts

Figure 3 illustrates the pin assignments of an RJ-45 connector and port.



**Figure 3** RJ-45 Connector and Port Pin Assignments

**Serial Port** The serial connection/management port features a DB-9 connector for connecting the access point to your laptop or PC-compatible computer for configuration using the provided management cable.

**Serial Cable** The RS-232 null-modem cable included with the AT-WL2411 access point features a 9-pin RS-232 connector to attach to the serial port on your computer and an 9-pin RS-232 connector to attach to the serial port on the access point.

**Power Supply Input Port** The access point has a single power supply port. The unit does not have a power switch. To turn the access point ON or OFF, you connect or disconnect the power cord.

**External AC/DC Power Adapter** An external AC/DC power adapter is included with the access point. The power adapter supplies 5V DC to the access point. The power required for the access point is 5V DC, 2.0 A.

## Firmware Features

---

The Version 1.72 firmware used to configure the AT-WL2411 access point has the following features:

- ☐ Remote access via Web browser, Telnet, and SNMP
- ☐ Configuration as a DHCP server or client
- ☐ Upgrades via serial port, Web browser, or Telnet
- ☐ Advanced filtering of wired data traffic
- ☐ Enhanced roaming reliability
- ☐ Load balancing

---

**Note**

The features listed here are further described in the **Configuration Overview** on page 39.

---

## Network Configurations

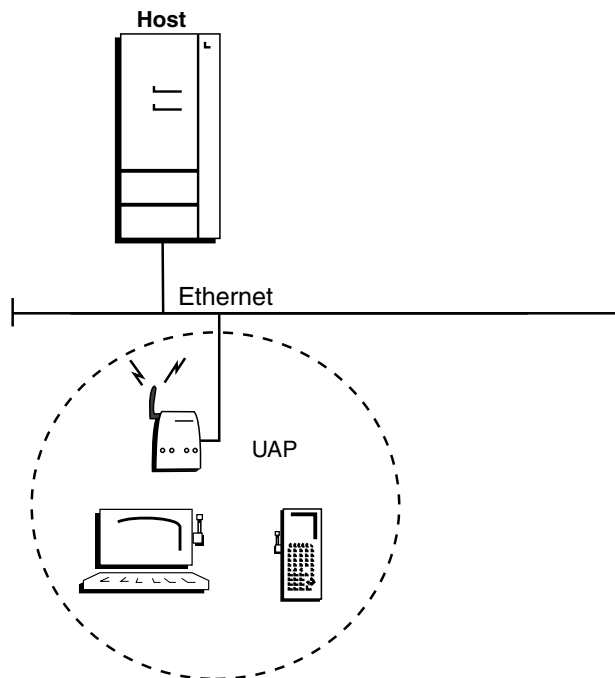
---

The AT-WL2411 access point supports a variety of network configurations that are explained in this section.

### A Simple Wireless Network

You can use the access point to extend your existing Ethernet network to include wireless end devices. The access point connects directly to your wired network and the end devices form a network that functions as a wireless extension of the wired LAN.

In a simple wireless network, a single access point on the wired network serves as a transparent bridge between the wired network and end devices. The end devices communicate exclusively with devices on the wired network; they do not communicate with other end devices. This kind of simple wireless network is illustrated in Figure 4.



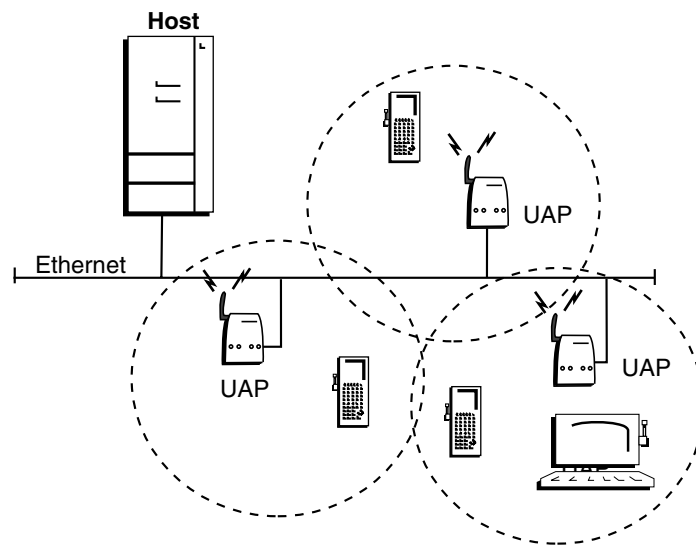
**Figure 4** Simple Wireless Network



## Using Multiple APs and Roaming End Devices

For larger or more complex environments, you can install multiple access points so end devices can roam from one access point to another. Multiple access points establish coverage areas or cells similar to those of a cellular telephone network. End devices can connect with any access point that is within range and belongs to the same network.

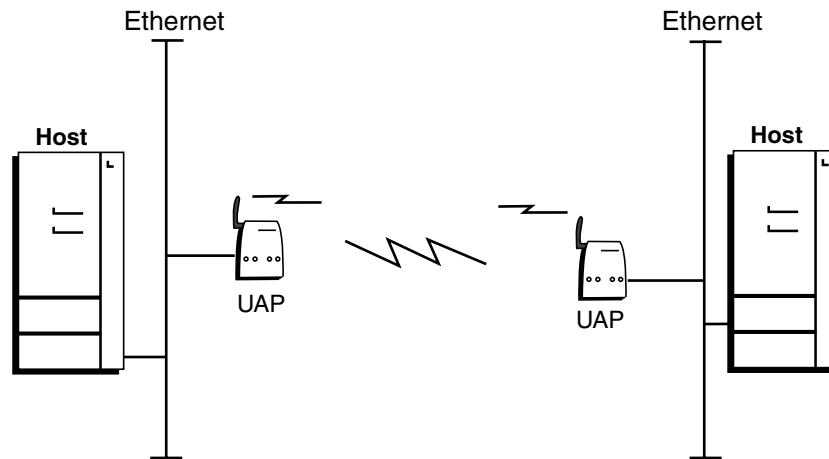
With the access point multichannel architecture, you can have more than one access point within the same cell area to increase throughput. In addition, overlapping radio coverage cells offer redundancy for critical applications so that coverage is not lost if a single access point or radio fails. This kind of network is illustrated in Figure 5.



**Figure 5** Multiple APs and Roaming End Devices

## Using APs to Create a Point-to-Point Bridge

You can use access points to create a wireless or point-to-point bridge between two LANs. You can have a access point wired to a network in one building and have a second access point wired to a network in another building. Wired clients in both buildings can then communicate with each other over the wireless bridge created by the access points. This configuration is useful in a campus environment where pavement or other objects prevent installation of a wired link. For information about configuring access points for point-to-point bridging, see [Configuring Wireless Hops](#). Figure 6 illustrates a network with a point-to-point bridge.



**Figure 6** APs as a Bridge Between Wired LANs

## Chapter 2

# Installation

---

This chapter contains the installation procedures for the access point. The installation process is described in the following sections:

- ☐ Installation Safety Precautions
- ☐ Selecting a Site for the Access Point
- ☐ Required Cables
- ☐ Unpacking the Access Point
- ☐ Installing the Access Point
- ☐ Attaching an External Antenna (Optional)
- ☐ Warranty Registration

## Installation Safety Precautions

---

Please review the following safety precautions before you begin to install the access point. Refer to **Translated Electrical Safety and Emission Information** on page 189 for translated safety statements in your language.



### Warning

**Power to the access point must be sourced only from the adapter:**

#### **Europe—EC**

Use TÜV licensed AC adapter of 5 V DC, min 2.0 A.

#### **Other Countries**

Use a Safety Agency Approved AC adapter of 5 V DC, min 2.0 A.  4

---




### Warning

**Power cord is used as a disconnection device:** To de-energize equipment, disconnect the power cord.  5

---




### Warning

**Lightning Danger:** Do not work on this equipment or cables during periods of lightning activity.  6

---




### Caution

**Air vents:** The air vents must not be blocked on the unit and must have free access to the room's ambient air for cooling.  7

---



### Caution

**Operating Temperature:** This product is designed for a maximum ambient temperature of 65°C.  8

---



### Caution

**All Countries:** Install this product in accordance with local and national electric codes.  9

---

## Selecting a Site for the Access Point

---

Allied Telesyn recommends that you have Allied Telesyn or other certified providers conduct a site survey to determine the ideal locations for all of your network components. A proper site survey requires special equipment and training.

Observe the following requirements when choosing a site for your access point:

- ☐ If you are installing the access point on a table, be sure that the table is level and secure.
- ☐ The power outlet for the access point should be located near the unit and should be easily accessible.
- ☐ The site should provide for easy access to the ports on the access point. This will make it easy for you to connect and disconnect cables.
- ☐ Try to position the access point so that its LEDs are visible. The LEDs are useful for troubleshooting.
- ☐ To allow proper cooling of the access point, air flow around the unit and through its vents on the side and rear should not be restricted.
- ☐ Do not place objects on top of the access point.
- ☐ Do not expose the access point to moisture or water.
- ☐ Make sure that the site is a dust-free environment.
- ☐ You should use dedicated power circuits or power conditioners to supply reliable electrical power to the access point.
- ☐ Locate access points centrally within areas requiring coverage.
- ☐ Overlap access point coverage areas to avoid coverage holes.
- ☐ Access points configured for the frequency in the same coverage area may interfere with each other and decrease throughput. You can reduce the chance of interference by configuring your access points so they are configured 5 channels apart, such as Channels 1, 6, and 11.
- ☐ Install wired LAN cabling within device limit and cable length limitations.
- ☐ Microwave ovens operate in the same frequency band as the 802.11b HR radio; therefore, if you use a microwave within range

of your Allied Telesyn RF network, you may notice network performance degradation. Both your microwave and your RF network will continue to function, but you may want to consider relocating your microwave out of range of your access point.

The access point features an advanced configuration parameter for the 802.11b HR radio called microwave oven robustness. You can enable this parameter to minimize potential interference between your microwave oven and your RF network.

## Cables Not Included

---

The AT-WL2411 access point requires the cables described in Table 2 below. These cables are not included with the access points.

**Table 2** Cables

Port	Cable	Connector
Ethernet	Category 3 or better 100-ohm unshielded straight-through or crossover twisted pair cable	RJ-45
Serial	RS-232 null-modem	RS-232

## Unpacking the Access Point

---

To unpack the access point:

1. Remove all components from the shipping package and store the packaging material in a safe location.

---

**Note**

You must use the original shipping material if you need to return the unit to Allied Telesyn.

---

2. Place the access point on a level, secure surface.
3. Make sure the following hardware components are included in your access point package. If any item is missing or damaged, contact your Allied Telesyn sales representative for assistance.
  - ☐ One AT-WL2411 access point
  - ☐ Mounting bracket
  - ☐ Power supply and AC power cord
  - ☐ Documentation CD



## Installing the Access Point

You can install the AT-WL2411 horizontally on a desk or counter, or you can install it vertically to a wall using the wall bracket that ships with it. An optional cubicle bracket is also available for mounting the AT-WL2411 on a cubicle wall.

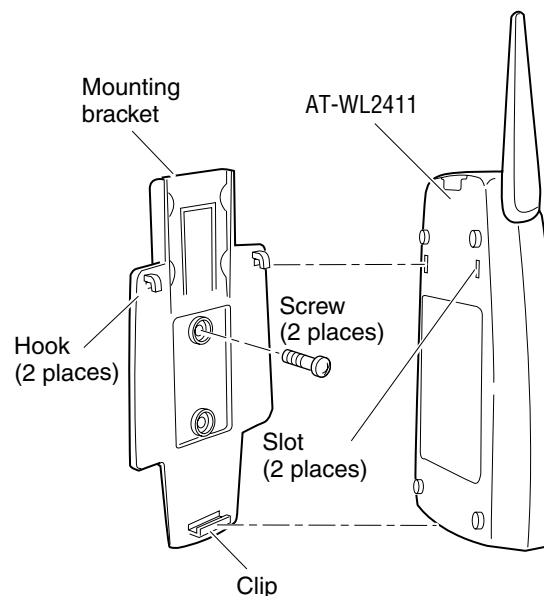
**Mounting** The following instructions explain how to mount the AT-WL2411 using the mounting bracket that ships with it.

To install the mounting bracket and AT-WL2411 on a sturdy surface in accordance with local building codes, you need the following tools and materials:

- ☐ Two #5 or M3 screws.
- ☐ Drill and drill bit appropriate for the mounting screws
- ☐ Screwdriver

To mount the AT-WL2411, do the following:

1. Use the mounting bracket as a template to mark the location of the mounting holes on the mounting surface.
2. Drill the mounting holes.
3. Position the bracket on the mounting surface
4. Using the screws you provided, secure the bracket to the wall, as shown in Figure 7.



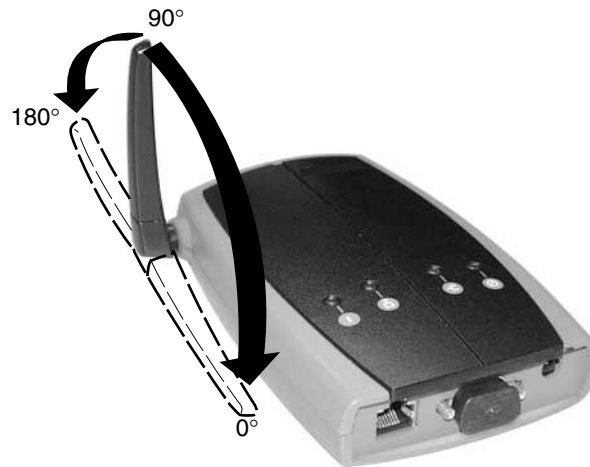
**Figure 7** Mounting

5. Fit the slots on the back of the AT-WL2411 over the hooks on the mounting bracket.
6. Slide the AT-WL2411 up slightly and then press the base of the AT-WL2411 until it clicks into the clip at the bottom of the mounting bracket.

## Positioning the Antenna

The AT-WL2411 features a built-in antenna that rotates 180° as shown in Figure 8. Use the following guidelines when positioning the antenna.

- ☐ Place the antenna at 0° when storing the AT-WL2411.
- ☐ Place the antenna at 90° when using the AT-WL2411 horizontally; for instance, when the AT-WL2411 is positioned on a desk or counter.
- ☐ Place the antenna at 180° when using the AT-WL2411 vertically; for instance, when the AT-WL2411 is mounted on a wall or cubicle.



**Figure 8** Positioning the Antenna

### Note

Do not force the antenna past the hard stop at 0° or 180° or you may break the antenna connector.

## Cabling

1. To cable the unit, first connect the Ethernet cable to the Ethernet port on the access point and then attach the other end of the cable to your Ethernet network.
2. To configure the access point or assign it an IP address for remote configuration, attach one end of the RS-232 null-modem management cable to the serial port on your access point and then attach the other end of the cable to the serial port on your computer. For instructions on how to further configure the access point, see **Configuration Overview** on page 39.

**Powering On**

Plug one end of the power cord into the power port on the access point and plug the other end into an AC power outlet to power ON the unit. The AT-WL2411 does not have a power switch, so it boots as soon as you apply power.

**Caution**

You must use the appropriate Allied Telesyn power supply with this device or equipment damage may occur.

---

Your AT-WL2411 is now ready to begin transmitting data packets between your end devices and your wired network.

## Attaching an External Antenna (Optional)

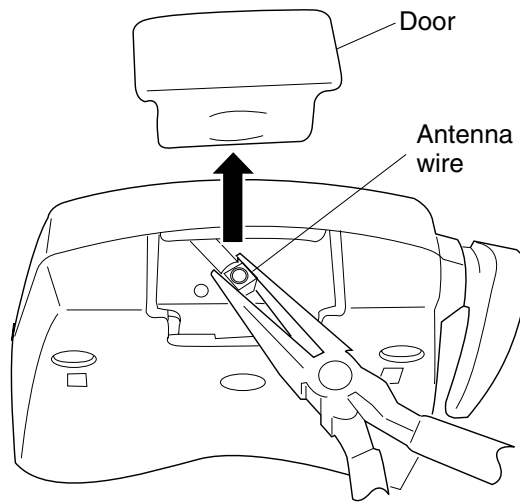
---

You can attach an external antenna to the AT-WL2411. To attach an external antenna, you must disconnect the built-in antenna and attach an antenna cable directly to the radio card in the access point. The following steps explain how to attach an antenna cable to the AT-WL2411.

For more information about antenna options, contact your local Allied Telesyn representative.

To attach an external antenna to the AT-WL2411, do the following:

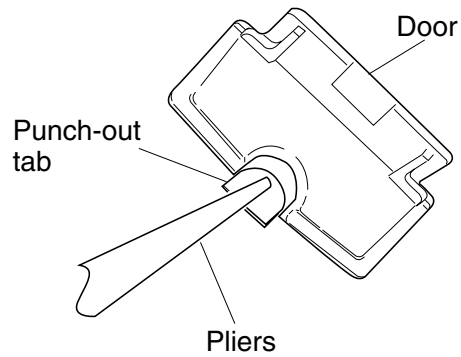
1. Remove the radio card door.
2. Pull straight up on the antenna wire to disconnect it from the radio card, as shown in Figure 9.



**Figure 9** Antenna Wire

3. Tuck the antenna wire inside the access point housing.

4. Remove the punch-out tab from the door, as shown in Figure 10.



**Figure 10** Punch-out Tab

5. Attach the antenna cable to the radio by inserting the cable connector into the radio card.
6. Replace the door.

## **Warranty Registration**

---

When you have finished installing the access point, register your product by completing the enclosed warranty card and mailing it to Allied Telesyn.

## Chapter 3

# Configuration Overview

---

The AT-WL2411 access point features four different management interfaces:

- ☐ Communications program via serial connection
- ☐ Telnet
- ☐ Web browser
- ☐ SNMP

---

**Note**

You must first access the management firmware using a communications program via serial connection to assign the access point an IP address before you can use the other management interface options. This manual assumes that most configurations will be performed remotely using a Web browser and provides in-depth instructions for configuration using a Web browser in later chapters.

---

## Using a Serial Connection

---

Although the AT-WL2411 access point will work directly out of the box, you must assign it an IP address and define other basic parameters before you can manage it remotely. To perform these initial configurations, you must use a serial connection and a terminal or a communications program (such as HyperTerminal). This manual assumes that you are using a communications program for your initial configuration and performing all other configurations remotely using the Web interface.

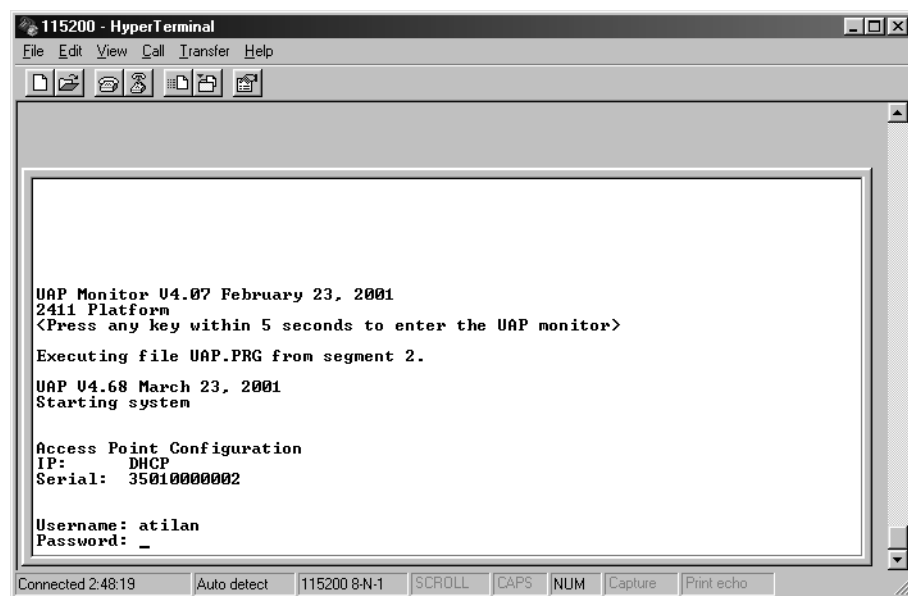
To perform a basic configuration of the AT-WL2411 using the default settings, you need the following:

- ☐ An RS-232 null-modem cable.
- ☐ A terminal or PC with an open serial port.

To configure the AT-WL2411:

1. Use the RS-232 null-modem cable to connect the serial port on the access point to a serial port on your PC.
2. Open your communications program and configure the serial communications parameters on your PC to:
 

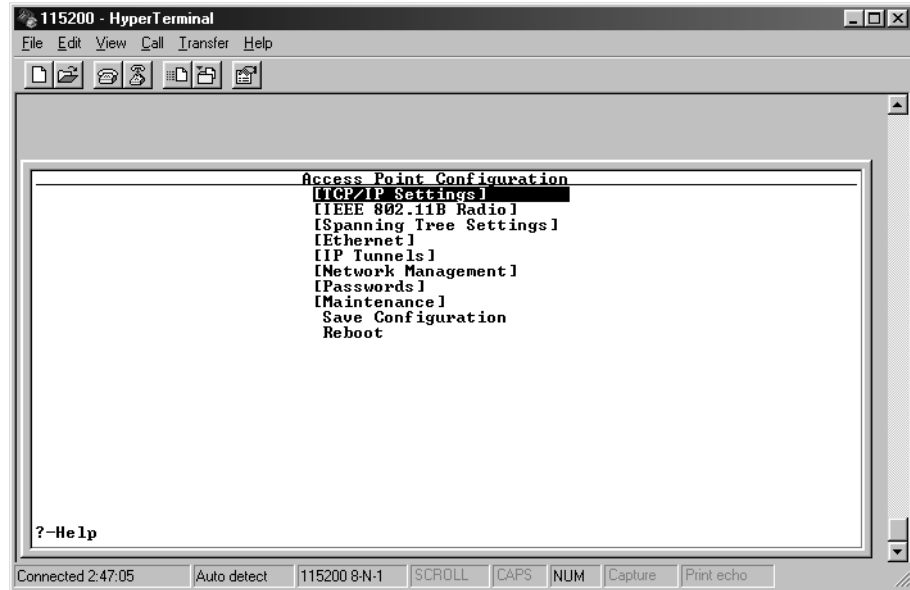
Baud	9600
Data bits	8
Parity	no
Stop bit	1
Flow control	none
3. Connect the power cable to the access point and to a power source. The access point does not have an On/Off switch, so the unit boots as soon as you apply power.
4. Press Enter when the message "Starting system" appears on your PC screen. The login screen appears, as shown in Figure 11.



**Figure 11** Login Screen



5. Type the default user name ATILAN and press Enter and then type the default password ATILAN and press Enter. The Configuration menu appears, as shown in Figure 12.



**Figure 12** Configuration Menu

6. To assign the access point an IP address so that you can continue configuration remotely, proceed to the next section **Assigning an IP Address** on page 42.

To continue configuration using the serial connection, use the menu shown in Figure 12.

7. When you have finished your configurations, save your changes by using the **Save Configuration** menu option and then reboot the access point to activate your changes.

## Assigning an IP Address

---

The AT-WL2411 will work directly out of the box if you are using a DHCP server to assign it an IP address. By default, the access point is configured to be a DHCP client. However, if you are not using a DHCP server to assign IP address, you must assign the access point an IP address before you can manage it remotely.

1. To use DHCP to automatically assign an IP address, configure the following parameters in the TCP/IP Settings menu:

### **DHCP Mode**

Set to <Use DHCP if IP Address is zero>.

### **DHCP Server Name**

The name of the DHCP server that the AT-WL2411 is to access for automatic address assignment. If no server name is specified, the AT-WL2411 responds to offers from any server.

To assign an IP address manually, configure these parameters in the TCP/IP Settings menu:

### **IP Address**

A unique IP address.

### **IP Subnet Mask**

The subnet mask that matches the other devices in your network.

### **IP Router (Gateway)**

The address of the router that will forward frames if the AT-WL2411 will communicate with devices on a subnetwork.

2. If you are configuring a AT-WL2411, you must configure Node Type in the Wireless Bridging submenu of the 802.11b Radio menu. Configure Node Type as Master if this radio will communicate with end devices; configure it as Station if you are configuring a WAP and this radio will communicate with an access point on the wired network.
3. In the Spanning Tree Settings menu, configure LAN ID (Domain). All access points must have the same LAN ID to participate in the same spanning tree.
4. In the 802.11b radio menu, configure these parameters:

### **(SSID) Network Name**

The network name. All 802.11b radios must have the same network name to communicate.

**Frequency**

The frequency appropriate for your installation. Frequencies range from 2.4 to 2.5 GHz and depend on the specific country.

5. Save the configurations by using the **Save Configuration** menu option and reboot the access point to activate your changes.

Now that the access point has an IP address, you can configure it remotely using the procedures in the next sections.

## Using a Web Browser

---

After you have configured the IP address and other basic network parameters as described in **Assigning an IP Address** on page 42, you can manage your access point using a Web browser.

You must know the IP address of the access point to manage it remotely. If a DHCP server assigned the IP address, you must determine the IP address from the DHCP server.

Only one session can be active on the access point at a time. If your session terminates abruptly or a new signon screen appears, someone else may be using the access point.

When using the Web to establish remote management of your access point, keep the following points in mind:

- ☐ Your session terminates if you do not use it for 15 minutes.
- ☐ Console Command mode is not available.

To establish a Web browser session with the access point, do the following:

1. Type the DHCP server-assigned IP address or the IP address you assigned to the access point in the address field of your Web browser.

---

**Note**

If you access the Internet using a proxy server, you must add the IP address to your exceptions list. The exceptions list contains the addresses that you do not want to use with a proxy server.

---

2. Press Enter. The Access Point Login screen appears, as shown in Figure 13.



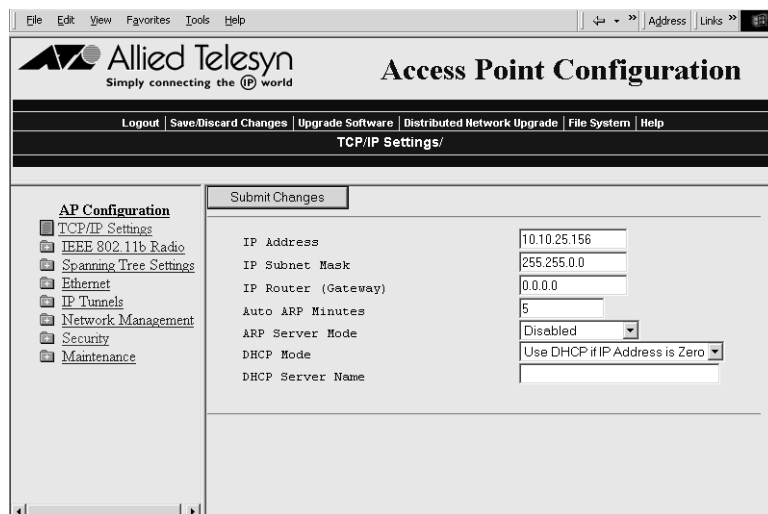
**Figure 13** Access Point Login Screen

3. Type **atilan** as both the default user name and default password.

### Note

You can change the user name and password on the Security menu.

4. Click Login. The TCP/IP Settings screen appears, as shown in Figure 14.



**Figure 14** TCP/IP Settings

You can now configure your access point using the Web browser menu.

## **Saving Your Configuration Changes**

---

There are two ways to save your configuration settings in a Web browser setting:

### **Submit Changes**

When you click Submit Changes, the access point updates the current configuration file. The access point does not change the active configuration file. You can see a list of pending changes when you click Save/Discard Changes. Having separate files for the current and active configurations lets you make changes while the access point is running without interrupting communication.

### **Save Discard/Changes**

When you click Save/Discard Changes and then you click Save Changes and Reboot, the access point copies the current configuration file to the active configuration file. The active configuration file is the file that the access point uses.

---

### **Note**

You must save your configuration changes and reboot the access point in order for the new configurations to become active.

---

## Using a Telnet Session

---

To establish a Telnet configuration session, you can:

1. Go to an MS-DOS prompt and type **Telnet IPaddress**, where *IPaddress* has the form *x.x.x.x* and *x* is a number from 0 to 255. Use the IP address assigned to the access point you want to configure.

OR

Open a Telnet program and type **open**. Press Enter. At the **<open>** prompt, type the IP address of the access point and press Enter.

2. Follow the configuration instructions in **Using a Serial Connection** on page 39, since the Telnet interface is similar to the communications program interface.

## Using SNMP

The access point supports SNMP management. Contact your Allied Telesyn representative for information about obtaining a copy of the MIB. The passwords for accessing the SNMP community table are shown below.

Type of Access	MIB Password
read only	public
read/write	CR52401

### Configuring the SNMP Community

Simple Network Management Protocol (SNMP) community strings are passwords used by SNMP. When you use an SNMP client, you must enter the correct community string to gain access to the access point SNMP interface.

To configure the SNMP community, do the following:

1. Establish a Web browser session if you have not already done so. For more information, see **Using a Web Browser** on page 44.
2. Click Network Management. The Community Strings screen appears, as shown in Figure 15.

Figure 15 shows the "Community Strings" configuration screen in the Allied Telesyn web interface. The page title is "Access Point Configuration". The navigation menu on the left includes "AP Configuration" and "Community Strings". The main content area displays three community strings: "SNMP Read Community", "SNMP Write Community", and "SNMP Secret Community". Each string has a corresponding input field with a masked password (represented by asterisks).

**Figure 15** Community Strings Screen



3. Configure the SNMP community parameters. When you are finished, click Submit Changes to save your changes.

The SNMP community parameters are explained below.

Parameter	Description
SNMP Read Community	Allows read-only access. Defaults to public.
SNMP Write Community	Allows read/write access. Defaults to CR52401.
SNMP Secret Community	Allows read/write access to change the community strings. Defaults to Secret.

## Chapter 4

# Configuring the Ethernet Network

---

This chapter explains how to configure the access point so that it communicates with your Ethernet network.

## Configuring the TCP/IP Settings

---

If you are using a DHCP server to automatically assign an IP address to the access point, go to **Configuring the Access Point as a DHCP Client** in the next section. If you are not using a DHCP server, you need to manually assign some TCP/IP parameters.

You should have already configured an IP address for the access point, as described in **Assigning an IP Address** on page 42.

To configure the TCP/IP settings:

1. From the menu, click TCP/IP Settings. The TCP/IP Settings screen appears, as shown in Figure 16.

The screenshot shows the Allied Telesyn Access Point Configuration web interface. The top navigation bar includes links for Logout, Save/Discard Changes, Upgrade Software, Distributed Network Upgrade, File System, and Help. The main title is "Access Point Configuration". Below the title, the "TCP/IP Settings/" page is displayed. On the left, a sidebar menu lists various configuration options: AP Configuration, TCP/IP Settings (selected), IEEE 802.11b Radio, Spanning Tree Settings, Ethernet, IP Tunnels, Network Management, Security, and Maintenance. The main content area features a "Submit Changes" button at the top left. Below it, a table of settings is shown:

IP Address	149.35.16.10
IP Subnet Mask	255.255.252.0
IP Router (Gateway)	149.35.16.1
Auto ARP Minutes	5
ARP Server Mode	Disabled
DHCP Mode	Use DHCP if IP Address is Zero
DHCP Server Name	CORPNET

**Figure 16** TCP/IP Settings

2. Configure the TCP/IP settings using the following parameters:

#### **IP Address**

Enter the IP address of the access point. The IP address has the form x.x.x.x, where x is a number from 0 to 225.

#### **IP Subnet Mask**

Enter the subnet mask that matches the other devices in your network. The subnet mask has the form x.x.x.x, where x is a number from 0 to 225.

#### **IP Router**

Enter the IP address of the router that will forward packets if the access point will communicate with devices on another subnet. The IP address has the form x.x.x.x, where x is a number from 0 to 225.

#### **IP Frame Type**

This parameter controls the encapsulation of IP frames sent by this access point. You select either DIX (Ethernet 2.0) or SNAP encapsulation.

**DIX**

Encapsulate using DIX (Ethernet 2.0) frames.

**SNAP**

Encapsulate using SNAP frames. You need to use SNAP if other network computers use SNAP encapsulation for IP frames.

3. If you want to configure the access point as a NAT server, see About Network Address Translation later in this section.

If you want to configure the access point as an ARP server, see Configuring the Access Point as an ARP Server later in this section.

If you want to configure the access point to send ARP requests, see Configuring the Access Point to Send ARP Requests later in this section.

If you want to configure the access point as a DHCP server, see **Configuring the Access Point as a DHCP Server** on page 53.

4. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## Configuring the Access Point as a DHCP Client

You can use a DHCP server to automatically assign an IP address to your access point; that is, the access point can act as a DHCP client.

---

**Note**

You cannot configure the access point as both a DHCP server and a DHCP client.

---

To configure the access point as a DHCP client:

1. From the menu, click TCP/IP Settings. The TCP/IP Settings screen appears, as shown in Figure 17.

**Figure 17** TCP/IP Settings

2. Click the down arrow on the right side of the DHCP Mode field and choose either "Always Use DHCP" or "Enabled, if IP Address is Zero." If you choose "Enabled, if IP Address is Zero, make sure that the IP Address field is 0.0.0.0.
3. In the DHCP Server Name field, enter the name of the DHCP server that the access point is to access for automatic address assignment. If no server name is specified, the access point responds to offers from any server.
4. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## Configuring the Access Point as a DHCP Server

You can configure the access point as a simple DHCP server that can provide DHCP server functions for small installations where no other DHCP server is available. The DHCP server will offer IP addresses to any DHCP client it hears as long as a pool of unallocated IP addresses is available. These clients may include other access points, wireless end devices, wired hosts on the distribution LAN, or wired hosts on secondary LANs.

**Note**

If you configure the access point as a DHCP server, it is not intended to replace a general purpose, configurable DHCP server, and it makes no provisions for synchronizing DHCP policy between itself and other DHCP servers. Customers with complex DHCP policy requirements should use other DHCP server software.

**Note**

You cannot configure the access point as both a DHCP server and a DHCP client.

To avoid a single point of failure, you can configure more than one access point to be a DHCP server; however, the access points do not share DHCP client databases. You should configure each DHCP server with a different DHCP address pool from which to allocate client addresses.

To configure the access point as a DHCP server:

1. From the menu, click TCP/IP Settings. The TCP/IP Settings screen appears, as shown in Figure 18.

The screenshot shows the 'Access Point Configuration' web interface for Allied Telesyn. The top navigation bar includes links for Logout, Save/Discard Changes, Upgrade Software, Distributed Network Upgrade, File System, and Help. The current page is 'TCP/IP Settings/'. On the left, a sidebar menu lists various configuration options, with 'TCP/IP Settings' selected. The main configuration area contains the following fields:

IP Address	149.35.16.10
IP Subnet Mask	255.255.252.0
IP Router (Gateway)	149.35.16.1
Auto ARP Minutes	5
ARP Server Mode	Disabled
DHCP Mode	Use DHCP if IP Address is Zero
DHCP Server Name	CORPNET

A 'Submit Changes' button is located at the top of the configuration area.

**Figure 18** TCP/IP Settings

2. Verify that the IP Subnet Mask field and IP Router field are configured. For help, see **Configuring the TCP/IP Settings** on page 50.

3. Click the down arrow on the right side of the DHCP Mode field and choose "This AP is a DHCP Server."
4. Click Submit Changes to save your changes.
5. Click DHCP Server Setup. The DHCP Server Setup screen appears, as shown in Figure 19.

The screenshot shows the Allied Telesyn Access Point Configuration web interface. The top header includes the Allied Telesyn logo and the text "Simply connecting the IP world". The main title is "Access Point Configuration". Below the title is a navigation bar with links: Logout, Save/Discard Changes, Upgrade Software, Distributed Network Upgrade, File System, and Help. The current page is "TCP/IP Settings/DHCP Server Setup/". On the left is a sidebar menu with "AP Configuration" expanded, showing sub-items: TCP/IP Settings, DHCP Server Setup (selected), IEEE 802.11b Radio, Spanning Tree Settings, Ethernet, IP Tunnels, Network Management, Security, and Maintenance. The main content area has a "Submit Changes" button at the top. Below it is a table of DHCP settings:

Low Address	10.10.10.100
High Address	10.10.10.199
DNS Address 1	0.0.0.0
DNS Address 2	0.0.0.0
Lease Time	0:0:20
IP Subnet Mask	255.255.255.0
IP Router (Gateway)	10.10.10.100
NAT Status	Auto-Enabled

**Figure 19** DHCP Server Setup

6. Configure the DHCP server using the following parameters:

#### **Low Address**

The low IP address in the range of IP addresses available to the DHCP server for distribution to DHCP clients. If these addresses are not on the same subnet as the access point, the access point will perform Network Address Translation (NAT) for the devices to which it grants IP addresses.

#### **High Address**

The high IP address in the range of IP addresses available to the DHCP server for distribution to DHCP clients. If these addresses are not on the same subnet as the access point, the access point will perform Network Address Translation (NAT) for the devices to which it grants IP addresses.

**DNS Address 1**

The IP address of a Domain Name Server that will be distributed to DHCP clients. You can enter up to two DNS addresses to be delivered to DHCP clients.

**DNS Address 2**

The IP address of a Domain Name Server that will be distributed to DHCP clients. You can enter up to two DNS addresses to be delivered to DHCP clients.

**Lease Time**

Specifies the duration of the leases that are granted by the DHCP server. Enter the lease time in the format days:hours:minutes. If you set the lease time to 0, infinite leases are granted

7. Click Submit Changes to save your changes and then click "here." To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

**Supported DHCP Server Options.**

The DHCP server issues IP address leases to configure this field:

**IP broadcast address**

The IP broadcast address, along with the subnet mask and IP router, will contain the same values as those configured for the access point.

**Unsupported DHCP Server Options.**

The DHCP server does not support any DHCP options other than those listed. The DHCP server disregards any DHCP options that are not explicitly required by the DHCP specification. The DHCP server ignores all packets with a non-zero giaddr (gateway IP address). The DHCP server only responds to requests from its own subnet.

## About Network Address Translation (NAT)

NAT allows IP addresses to be used by more than one device. The access point can act as a NAT server, which instantaneously rewrites IP addresses and port numbers in IP headers so that packets all appear to be coming from (or going to) the single IP address of the access point instead of the actual source or destination.

When a device uses the access point as an IP router, the access point replaces the IP header, which includes the device's MAC address, IP source address, and TCP/UDP port, with its own. You can configure the DHCP server to indicate that the access point is the IP router when the



server allocates an IP address. Special consideration is given to changing the FTP data connection TCP port number, which is in the body of the TCP packet. After the packet source is modified, it is forwarded to the proper subnet.

If the destination subnet is not the same subnet as the access point's Ethernet network, the destination MAC address is changed to the IP router that has been configured for the access point. If destination subnet is the same subnet as the access point's Ethernet network, the access point converts the MAC address to the MAC address that belongs to the destination IP address. This may involve using ARP for MAC address discovery.

When the access point receives a packet with its IP address, it identifies the need for address translation by inspecting the destination port number. If the port number is within the pool reserved for NAT operation, it looks up the original MAC address, IP address, and port number. The packet is then modified and forwarded to the end device.

NAT operation is disabled or enabled automatically depending on the continuous range of addresses you enter into the DHCP server. NAT is disabled if the range of addresses to be given to DHCP clients is on the same subnet as the access point. NAT is enabled if the range of addresses to be given to DHCP clients is not on the same subnet as the access point; thus, you are creating a virtual network and the DHCP server will also perform NAT translation.

When NAT operation is enabled, the access point uses the low address in the range of addresses as its own. The DHCP/NAT clients also use this address as their router IP address. These clients can configure the access point using this internal IP address or the normal external IP address.

To configure the access point as a NAT server:

1. From the menu, click TCP/IP Settings. The TCP/IP Settings screen appears, as shown in Figure 16.

The screenshot shows the Allied Telesyn Access Point Configuration web interface. The header includes the Allied Telesyn logo and the text "Simply connecting the IP world". The main title is "Access Point Configuration". Below the title is a navigation bar with links: Logout, Save/Discard Changes, Upgrade Software, Distributed Network Upgrade, File System, and Help. The current page is "TCP/IP Settings/". On the left is a sidebar menu with "AP Configuration" and sub-items: TCP/IP Settings (selected), IEEE 802.11b Radio, Spanning Tree Settings, Ethernet, IP Tunnels, Network Management, Security, and Maintenance. The main content area has a "Submit Changes" button at the top. Below it is a table of settings:

IP Address	149.35.16.10
IP Subnet Mask	255.255.252.0
IP Router (Gateway)	149.35.16.1
Auto ARP Minutes	5
ARP Server Mode	Disabled
DHCP Mode	Use DHCP if IP Address is Zero
DHCP Server Name	CORPNET

**Figure 20** TCP/IP Settings

2. Verify that the IP Address field and IP Subnet Mask field are configured. For help, see **Configuring the TCP/IP Settings** on page 50.
3. Click the down arrow on the right side of the DHCP Mode field and choose "This AP is a DHCP Server."
4. Click Submit Changes to save your changes.
5. Click DHCP Server Setup and enter a range of IP addresses that are NOT on the same subnet as the access point.
6. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

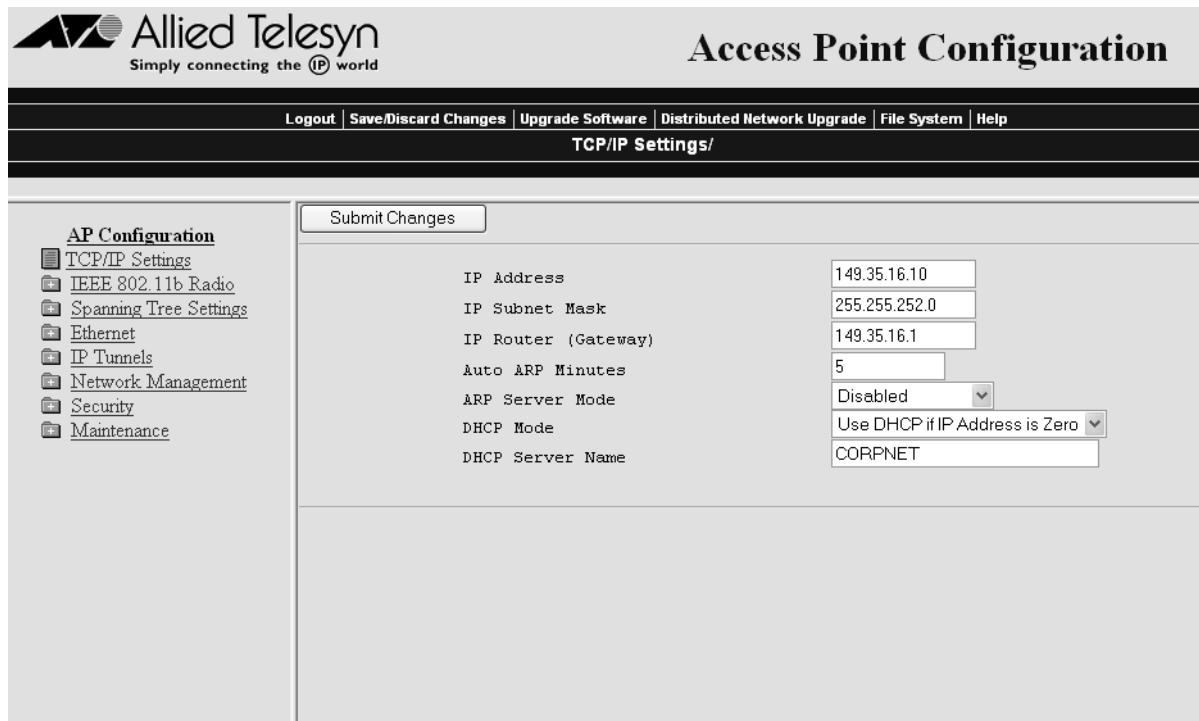
## Configuring the Access Point as an ARP Server

The access point maintains an ARP cache, which is a table of known MAC addresses and associated IP addresses. When an access point receives an ARP request on its Ethernet port, it checks its ARP cache to determine if the destination IP address is known. If the destination IP address is known and you have enabled ARP Server mode, the access point will act as an ARP server.

An ARP request is a multicast packet, which means the packet is sent to all devices on the network. If the access point is acting as an ARP server, it translates the multicast packet into a unicast packet, which means that the packet is only sent to the destination end device. Thus, all wireless end devices do not need to wake up to listen to the ARP request, which saves battery life.

To configure the access point as an ARP server:

1. From the menu, click TCP/IP Settings. The TCP/IP Settings screen appears, as shown in Figure 21.



**Allied Telesyn**  
Simply connecting the IP world

## Access Point Configuration

Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File System | Help

### TCP/IP Settings/

Submit Changes

IP Address	149.35.16.10
IP Subnet Mask	255.255.252.0
IP Router (Gateway)	149.35.16.1
Auto ARP Minutes	5
ARP Server Mode	Disabled
DHCP Mode	Use DHCP if IP Address is Zero
DHCP Server Name	CORPNET

**Figure 21** TCP/IP Settings

2. Click the down arrow on the right side of the ARP Server Mode field and choose No Flooding or Normal Flooding.
3. To disable the ARP server, choose Disabled.
4. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## Configuring the Access Point to Send ARP Requests

ARP requests are multicast packets, which means they are sent to all devices on the network. The access point periodically sends an unsolicited ARP request to the default IP router so that all routers can update their routing tables. This ARP request enables a network management program to learn about the access point on the network by querying routers. The auto ARP period controls the time interval between ARP broadcasts.

If the address of the default IP router is 0.0.0.0, the access point sends an ARP request to its own IP address. Without this option, an access point might not use its IP address for extended periods of time and the IP address would expire from the router ARP table. If the IP address expires, the network management program must ping all potential addresses on a subnet to locate active IP addresses or require the user to enter a list. You should not let the IP address for the access point expire.

To set the auto ARP period:

1. From the menu, click TCP/IP Settings. The TCP/IP Settings screen appears, as shown in Figure 22.

The screenshot displays the 'Access Point Configuration' web interface for Allied Telesyn. The top navigation bar includes links for Logout, Save/Discard Changes, Upgrade Software, Distributed Network Upgrade, File System, and Help. The main content area is titled 'TCP/IP Settings/' and features a 'Submit Changes' button. On the left, a sidebar lists configuration categories: AP Configuration, TCP/IP Settings (selected), IEEE 802.11b Radio, Spanning Tree Settings, Ethernet, IP Tunnels, Network Management, Security, and Maintenance. The main configuration area contains the following fields:

IP Address	149.35.16.10
IP Subnet Mask	255.255.252.0
IP Router (Gateway)	149.35.16.1
Auto ARP Minutes	5
ARP Server Mode	Disabled
DHCP Mode	Use DHCP if IP Address is Zero
DHCP Server Name	CORPNET

**Figure 22** TCP/IP Settings

2. In the Auto ARP Minutes field enter a time period from 1 to 120 minutes. To disable this parameter, set the time period to 0.

3. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## Configuring the Ethernet Settings

---

Many of the standard Ethernet settings are configured in the TCP/IP Settings screen. For help, see **Configuring the TCP/IP Settings** on page 50. In the Ethernet Settings screen, you can

- ☐ Set the port type, if you have both an Ethernet port and a fiber optic port. This field specifies the port that the access point uses to communicate with the Ethernet network. If you do not have a fiber optic port, you will not see this field.
- ☐ Set the link speed, if you chose the port type to be Ethernet. This field specifies the speed and the duplex mode that the access point uses to communicate with the Ethernet network. If you chose the port type to be fiber optic, the link speed is automatically set to 100 Mbps Fiber Optic. If you want the access point to auto-negotiate this field, choose Auto Select. Auto Select is the default setting and should work for most networks.
- ☐ Enable or disable the link status check. Enable this parameter if you want the access point to periodically check its Ethernet connection. If it loses the connection, this access point can no longer be the root access point and any end devices that are connected to this access point (whether or not it is the root) will roam to a different access point. The access point will attempt to reconnect to the spanning tree through one of its radio ports. Disable this parameter if this access point must be the root access point or if it is used as a WAP.
- ☐ Set the hello period, which defines how often the access point sends out multicast hello packets so it can dynamically discover and test connections to other routers on the network. Once this information is learned, the access point and routers can exchange routing information.

To configure the Ethernet or fiber optic settings:

1. From the menu, click Ethernet. The Ethernet screen appears, as shown in Figure 23.

The screenshot displays the Allied Telesyn Access Point Configuration web interface. At the top, the Allied Telesyn logo and tagline 'Simply connecting the IP world' are on the left, and the title 'Access Point Configuration' is on the right. Below the title is a navigation bar with links: Logout, Save/Discard Changes, Upgrade Software, Distributed Network Upgrade, File System, and Help. The 'Ethernet/' section is highlighted in the navigation bar. On the left side, there is a sidebar menu titled 'AP Configuration' with a tree view containing the following items: TCP/IP Settings, IEEE 802.11b Radio, Spanning Tree Settings, Ethernet (selected), Address Table, Frame Type Filters, Predefined Subtype Filter, Customizable Subtype Filter, Advanced Filters, IP Tunnels, Network Management, Security, and Maintenance. The main content area features a 'Submit Changes' button at the top. Below it, the 'Hello Period' is displayed as a text field with a dropdown arrow, currently set to '2 Seconds'.

**Figure 23** Ethernet

2. Click down arrow on the right side of the Hello Period field and choose a hello period of 1, 2, or 3 seconds.
3. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## Configuring Ethernet Filters

---

You can set both Ethernet and IP tunnel filters, and you can create protocol filters for both predefined and user-defined protocol types. In addition, you can define arbitrary frame filters based on frame content.

For help with configuring IP filters, see **Configuring IP Tunnel Filters** on page 98.

### Configuring the Ethernet Address Table

You can use the Ethernet address table to list the permanent unicast 802 MAC addresses that are using the access point that is the designated bridge on the secondary LAN to communicate to the primary LAN. These addresses become permanent entries in the route table of the designated bridge on the secondary LAN.

You must enter the MAC addresses of the devices on the secondary LAN that do not **always** initiate communication.

You should fill in this table when configuring designated bridges for secondary LANs so that this access point will not need to flood frames to all the wired stations on the secondary LAN. If you choose not to use this table, the access point may need to flood frames to all ports (Ethernet and radio) to learn the path to the MAC address.

To configure the Ethernet address table:

1. From the main menu, click Ethernet and then click Ethernet Filters.



2. Click Address Table. The Address Table screen appears, as shown in Figure 24.

The screenshot shows the 'Access Point Configuration' web interface. The top navigation bar includes links for Logout, Save/Discard Changes, Upgrade Software, Distributed Network Upgrade, File System, and Help. Below this is the 'Ethernet/Address Table/' section. The left sidebar lists various configuration options, with 'Address Table' selected. The main content area shows a table with 16 rows, each containing a number (1-16) and a MAC address field (00:00:00:00:00:00). A 'Submit Changes' button is located at the top left of the table area.

**Figure 24** Address Table

3. Enter up to 20 MAC addresses. MAC addresses consist of six hex pairs that are separated by spaces, colons, or hyphens.
4. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## Using Ethernet Frame Type Filters

You can define filters for common networking protocols such as IP, Novell IPX, and 802.2 LLC. You can also set filters that will pass only those Ethernet frame types found on your network.

You can set the default action for general and specific frame types. For example, you can set the DIX-Other EtherTypes frame parameter to drop, and then use the subtype menus to pass only those specific DIX types that are used in your radio network.

You can also set the scope for general and specific frame types. For example, you can set the action to Drop and the scope to All for DIX-IP-TCP Ports, and then all IP packets with the TCP type will be dropped even if specific TCP parts are set to pass in the subtype menus.

**Action**

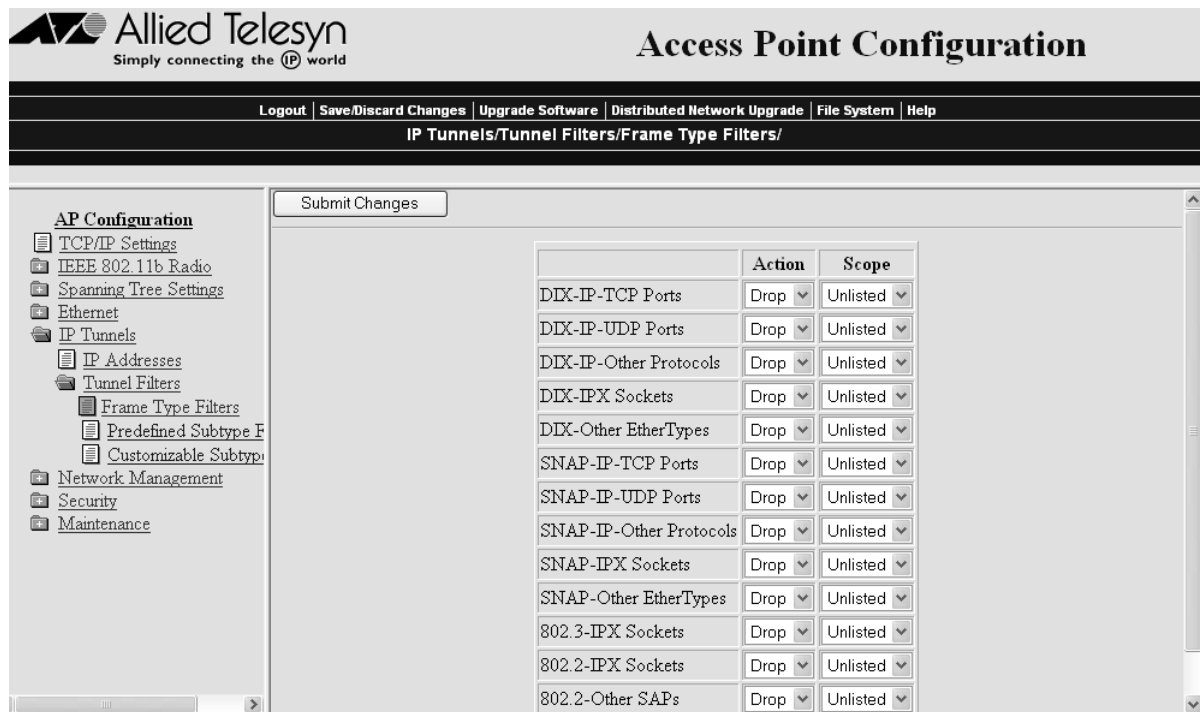
Set the action to Pass or Drop. If you select Pass, then all frames of that type are passed. If you select Drop, then all frames of that type are dropped.

**Scope**

Set scope to Unlisted or All. If you select All, then all frames of that type are unconditionally passed or dropped, depending on the action you specified. If you select Unlisted, then frames are passed or dropped only if the frame type is not listed in the predefined or customizable tables.

To set frame type filters:

1. From the main menu, click Ethernet and then click Frame Type Filters. The Frame Type Filters screen appears, as shown in Figure 25.



**Figure 25** Frame Type Filters

2. In each frame type field, click the down arrow on the right side of the Action field and set the action to Pass or Drop.
3. In each frame type field, click the down arrow on the right side of the Scope field and set the scope to Unlisted or All.

---

**Note**

If you set the Scope field to Unlisted for any of the frame types, you must also configure predefined subtype filters or customizable subtype filters. For help, see **Using Predefined Subtype Filters** on page 68 or **Customizing Subtype Filters** on page 68.

---

The various frame types are explained below:

**DIX IP TCP Ports****DIX IP UDP Ports****SNAP IP TCP Ports****SNAP IP UDP Ports**

Primary Internet Protocol Suite (IP) transport protocols.

**DIX IP Other Protocols****SNAP IP Other Protocols**

IP protocols other than TCP or User Datagram Protocol (UDP).

**DIX IPX Sockets**

Novell NetWare protocol over Ethernet II frames.

**SNAP IPX Sockets**

Novell NetWare protocol over 802.2 SNAP frames.

**802.3 IPX Sockets**

Novell NetWare protocol over 802.3 RAW frames.

**DIX Other Ethernet Types****SNAP Other Ethernet Types**

DIX or SNAP registered protocols other than IP or IPX.

**802.2 IPX Sockets**

Novell running over 802.2 Logical Link Control (LLC).

**802.2 Other SAPs**

802.2 SAPs other than IPX or SNAP.

---

**Note**

You cannot filter HTTP, Telnet, SNMP, and ICMP frames because they are used for configuration and management of the access point. Additionally, you cannot filter broadcast ARP request packets if the target IP address belongs to the local access point or to an access point in the subtree rooted at the local access point.

---

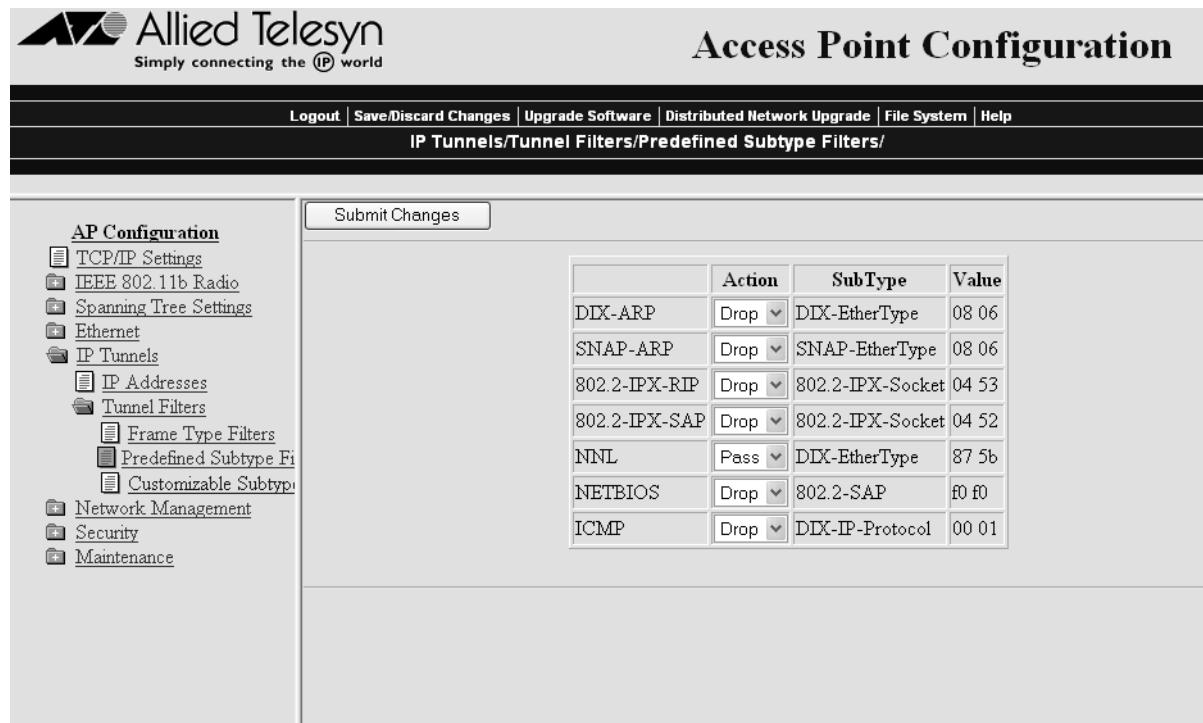
4. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## Using Predefined Subtype Filters.

You can configure the access point to pass or drop certain predefined frame subtypes.

To configure predefined subtype filters:

1. From the main menu, click Ethernet and then click Predefined Subtype Filters. The Predefined Subtype Filters screen appears, as shown in Figure 26.



**Figure 26** Predefined Subtype Filters

2. In each frame subtype field, click the down arrow on the right side of the Action field and choose Pass or Drop.
3. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## Customizing Subtype Filters.

You can configure the access point to pass or drop certain customized frame subtypes. You define the action, subtype, and value parameters.

**Action**

Set the action to Pass or Drop. If you select Pass, then all frames of that subtype and value are passed. If you select Drop, then all frames of that subtype and value are dropped.

**Subtype**

Selects the frame subtype you wish to configure.

**Value**

The following table describes frame subtypes and their values. The value must be two hex pairs. You must enter port values as decimals; for example, enter "23." for port 23. The access point displays the hexadecimal equivalent in the Value field on the menu. When a match is found between frame subtype and value, the specified action is taken.

To customize subtype filters:

1. From the main menu, click Ethernet and then click Customizable Subtype Filters. The Customizable Subtype Filters screen appears, as shown in Figure 27.

**Access Point Configuration**

Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File System | Help

IP Tunnels/Tunnel Filters/Customizable Subtype Filters/

**AP Configuration**

- TCP/IP Settings
- IEEE 802.11b Radio
- Spanning Tree Settings
- Ethernet
  - IP Tunnels
  - IP Addresses
  - Tunnel Filters
    - Frame Type Filters
    - Predefined Subtype F
    - Customizable Subtype
- Network Management
- Security
- Maintenance

Submit Changes

	Action	SubType	Value
1	Drop	DIX-IP-TCP-Port	00 00
2	Drop	DIX-IP-TCP-Port	00 00
3	Drop	DIX-IP-TCP-Port	00 00
4	Drop	DIX-IP-TCP-Port	00 00
5	Drop	DIX-IP-TCP-Port	00 00
6	Drop	DIX-IP-TCP-Port	00 00
7	Drop	DIX-IP-TCP-Port	00 00
8	Drop	DIX-IP-TCP-Port	00 00
9	Drop	DIX-IP-TCP-Port	00 00
10	Drop	DIX-IP-TCP-Port	00 00
11	Drop	DIX-IP-TCP-Port	00 00
12	Drop	DIX-IP-TCP-Port	00 00

**Figure 27** Customizable Subtype Filters

2. Click the down arrow on the right side of the Action field and choose Pass or Drop.
3. Click the down arrow on the right side of the SubType field and choose the customizable frame subtype.

4. Click the down arrow on the right side of the Value field and enter the two hex pairs. The frame subtype filters and their values are defined below.

**DIX-IP-TCP-Port**

Port value in hexadecimal.

**DIX-IP-UDP-Port**

Port value in hexadecimal.

**DIX-IP-Protocol**

Protocol number in hexadecimal.

**DIX-IPX-Socket**

Socket value in hexadecimal.

**DIX-EtherType**

Specify the registered DIX type in hexadecimal.

**SNAP-IP-TCP-Port**

Port value in hexadecimal.

**SNAP-IP-UDP-Port**

Port value in hexadecimal.

**SNAP-IP-Protocol**

Port value in hexadecimal.

**SNAP-IPX-Socket**

Socket value in hexadecimal.

**SNAP-EtherType**

SNAP type in hexadecimal. To filter on both SNAP type and OUI, use advanced filters.

**802.3-IPX-Socket**

Socket value in hexadecimal.

**802.2-IPX-Socket**

Socket value in hexadecimal.

**802.2-SAP**

802.2 SAP in hexadecimal.

5. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## Configuring Advanced Filters

You can configure advanced filters if you need more flexibility in your filtering. Settings for advanced filters execute after those for other filters; that is, advanced filters are only applied if the frame has passed the other filters.

You can use filter values and filter expressions to minimize network traffic over the wireless links; however, it is recommended that you use advanced Ethernet filters only if you have an extensive understanding of network frames and their contents. Use other existing filters whenever possible.

### Setting Filter Values.

You can associate an ID with a pattern value by selecting a filter and then entering an ID and a value. All values with the same value ID belong to the same list.

To set the value ID and value:

1. From the main menu, click Ethernet and then click Advanced Filters.
2. Click Filter Values. The Filter Values screen appears, as shown in Figure 28.

Access Point Configuration

Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File System | Help

Ethernet/Advanced Filters/Filter Values/

Submit Changes

	Value ID	Value
1	0	
2	0	
3	0	
4	0	
5	0	
6	0	
7	0	
8	0	
9	0	
10	0	
11	0	
12	0	

**Figure 28** Filter Values

3. Enter up to 22 value IDs and values.

- Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

### Setting Filter Expressions.

You can set filter expressions by specifying parameters for packet filters. You can also create a filter expression, which is executed in ascending order based on the ExprSeq values until the access point determines whether to pass or drop the frame.

To set filter expressions:

- From the main menu, click Ethernet and then click Advanced Filters.
- Click Filter Expressions. The Filter Expressions screen appears, as shown in Figure 29.

**Allied Telesyn**  
Simply connecting the IP world

**Access Point Configuration**

Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File System | Help

Ethernet/Advanced Filters/Filter Expressions/

Submit Changes

	ExprSeq	Offset	Mask	Op	Value ID	Action
1	0	0		EQ	0	And
2	0	0		EQ	0	And
3	0	0		EQ	0	And
4	0	0		EQ	0	And
5	0	0		EQ	0	And
6	0	0		EQ	0	And
7	0	0		EQ	0	And
8	0	0		EQ	0	And
9	0	0		EQ	0	And
10	0	0		EQ	0	And
11	0	0		EQ	0	And
12	0	0		EQ	0	And

**Figure 29** Filter Expressions

- Configure the filter expressions parameters. The filter expressions parameters are defined below.

#### ExprSeq (Expression Sequence)

Chains expressions together for filtering. After you change the parameter, the statements are reordered and renumbered so the Expression Sequence order is maintained. The range is from 0 to 255.



This parameter works with the Action parameter; for example, if the action is set to And, then the next sequence in another expression is processed.

### **Offset**

Identifies a point inside a bracket where testing for the expression is to start. The range is from 0 to 65535.

### **Mask**

Applies a data pattern to the packet. If the data pattern in the mask matches the packet, then the specific action is performed. The mask indicates the bits that are significant at the specified offset. A bit is significant if a bit in the mask is set to one. If this field is empty, the length of the field is determined by the longest value in the Filter Values menu for the specified value ID. The mask values are entered in hexadecimal pairs. You can enter 0 to 8 pairs.

### **Op (Operation)**

Performs a logical operation when a data pattern matches a value in the Filter Values menu to determine if the specified action should be taken. Valid operations include:

- ☐EQ (equal)
- ☐NE (not equal)
- ☐GT (greater than)
- ☐LT (less than or equal)

### **Value ID**

Represents a value in the Filter Values menu. The bytes after the packet offset are compared to the data pattern indicated by the value. Value ID can be from 0 to 255 and must match one or more value IDs in the Filter Values menu.

### **Action**

Sets the action to Pass, Drop, or And. If you set the action to And, the filter expression with the next highest sequence is applied.

4. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## Chapter 5

# Configuring the Spanning Tree

---

This chapter explains how to configure the spanning tree parameters, global flooding parameters, and global RF parameters. It also explains how to configure IP tunnels and IP tunnel filters.

## Configuring the Spanning Tree Parameters

---

Access points automatically configure themselves into a self-organized network using a spanning tree topology. As devices are added to or removed from the network, the access points automatically reconfigure to maintain reliable operation. The spanning tree provides efficient, loop-free forwarding of frames through the network and allows rapid roaming of wireless end devices.

To configure the spanning tree parameters:

1. From the menu, click Spanning Tree Settings. The Spanning Tree Settings screen appears, as shown in Figure 30.

**Allied Telesyn**  
Simply connecting the IP world

**Access Point Configuration**

Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File System | Help

**Spanning Tree Settings/**

**AP Configuration**

- TCP/IP Settings
- IEEE 802.11b Radio
- Spanning Tree Settings**
  - Global Flooding
  - Global RF Parameters
- Ethernet
- IP Tunnels
- Network Management
- Security
- Maintenance

Submit Changes

AP Name	21210100039j
LAN ID (Domain)	0
Root Priority	1
Ethernet Bridging	Enabled
Secondary LAN Bridge Priority	0
Secondary LAN Flooding	Disabled

**Figure 30** Spanning Tree Settings

2. Configure the spanning tree parameters. The spanning tree parameters are defined below.

#### **AP Name**

Enter a unique name for this access point. The name can be from 1 to 16 characters. The default is the access point serial number.

#### **LAN ID (Domain)**

Enter the LAN ID. All access points must have the same LAN ID to participate in the same spanning tree. The LAN ID can be from 0 to 254.

Also, if you assign a LAN ID greater than 15, the access point uses a LAN ID that is the remainder after dividing the LAN ID by 16. For example, if you set the LAN ID to 21 or 37, the access point uses 5.

#### **Root Priority**

Determines if this access point is a candidate to become the root of the spanning tree. The access point with the highest root priority becomes the root whenever it is powered on and active.

The root priority can be a value from 0 to 7. If you set the root priority to 0, the access point can never become the root access point. You should always set a WAPs root priority to 0.

For more information, see “About the Root Access Point” later in this section.

### **IAPP Frame Type**

Controls the encapsulation of Inner Access Point Protocol (IAPP) frames sent by this access point. You can select either DIX (Ethernet 2.0) or SNAP encapsulation. Choose SNAP if other network computers use SNAP encapsulation for IP frames.

### **Ethernet Bridging**

Determines how wireless frames are converted to Ethernet frames and vice versa.

#### **Enabled**

Choose Enabled if you want frames to be forwarded directly to the Ethernet network. On the root access point, this parameter is always enabled.

#### **Disabled**

Choose Disabled to use data link tunneling. The access point forwards data from the wireless network encapsulated in OWL data frames to the root access point. The root access point unencapsulates these frames and dumps them raw on the Ethernet network. Also, the root access point encapsulates all Ethernet traffic that is sent to the wireless network. When access points receive this traffic, they forward it to the wireless network. This process makes it seem like all wireless traffic is originating on the root access point's switch port. You may need to use data link tunnels to make roaming transparent to network protocols that are not designed to accommodate roaming.

### **Secondary LAN Bridge Priority**

Determines when and if the access point can become the designated bridge in a secondary LAN. To become a designated bridge, the access point must have at least one radio configured as a Station node or be the endpoint of an IP tunnel. The access point that meets either one of these requirements and has the highest secondary LAN bridge priority will be the designated bridge.

The secondary LAN bridge priority can be a value from 0 to 7. If you set the priority to 0, wireless traffic is encapsulated and will use data link tunneling to the secondary LAN bridge. The secondary LAN bridge will then forward the data to the primary LAN.

For more information, see “About Secondary LANs and Designated Bridges” later in this section.

### **Secondary LAN Flooding**

When an access point is the designated bridge in a secondary LAN, this parameter specifies the types of frames it passes from the primary LAN to the secondary LAN.

#### **Disabled**

No flooding occurs unless the root access point (in the Global Flooding screen) enables the Multicast or Unicast Outbound to Secondary LANs parameter.

#### **Enabled**

Multicast and unicast flooding occurs unless the root access point (in the Global Flooding screen) disables multicast or unicast flooding.

#### **Multicast**

Multicast flooding occurs unless the root access point (in the Global Flooding screen) disables multicast flooding.

#### **Unicast**

Unicast flooding occurs unless the root access point (in the Global Flooding screen) disables unicast flooding.

3. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## **About the Root Access Point**

The root access point is always on the primary LAN and initiates the spanning tree. The root coordinates the network and distributes global system parameters to other access points. The root is elected from a group of access points that are designated as root candidates (access points that are powered on, active, and do not have a root priority of 0). The access point with the highest root priority is the root.

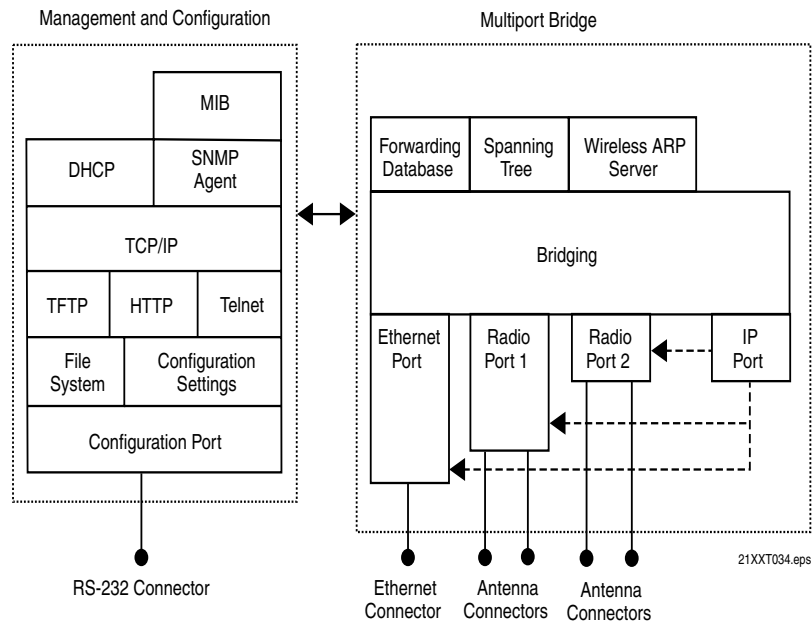
The election process also occurs in the event of a root access point failure. Besides the root, you should have two or three access points with a non-zero root priority. If two access points have the same root priority, the access point with the highest Ethernet address becomes the root. You should configure your network with overlapping coverage so that the network can automatically recover from any single point of failure.

After the root access point is elected, it transmits hello messages on all enabled ports. The spanning tree forms as other access points receive hello messages and attach to the network on the optimal path to the root. A non-root access point also transmits hello messages after it is

attached to the network. Each hello message contains the LAN ID of the access point that originated the message. The protocol does not allow wireless links to exist between access points that do not have matching LAN IDs.

## About Bridging

Wireless end devices operate similarly to other Ethernet products; therefore, all of your existing Ethernet applications will work with the wireless network without any special networking software. Figure 31 shows the general architecture of the access point.



**Figure 31** General Architecture of the Access Point

By default, wireless traffic is not bridged to a remote IP subnet. Any access point on a remote subnet that can receive IP hello messages can establish an IP tunnel; therefore, multiple IP tunnels can exist between the root access point and a single remote IP subnet.

If bridging is disabled, all traffic for end devices is forwarded between access points using data link encapsulation, which means that the MAC source/destination addresses correspond to the access points originating/receiving the traffic for the end devices. By using data link encapsulation, you prevent network monitoring tools and other network components from detecting end device MAC/IP addresses that belong to the remote subnet. It is strongly recommended that you use the default setting when you are using IP tunnels to provide mobility of other routable protocols, such as IPX. In some network installations, detecting these addresses may generate alarms or cause switches to behave erroneously. There is no additional forwarding overhead for disabling bridging in this situation.

If you enable bridging on a remote subnet, a single access point functions as the designated bridge for the secondary LAN. In this case, only the designated bridge can establish an IP tunnel. Any other access point on the remote subnet must attach to the network through the designated bridge. End device MAC/IP addresses are fully visible on the remote subnet. If you are using IP tunnels to provide mobility for IP and other non-routable protocols, you can enable bridging on remote IP subnets, because IP has built-in safeguards and filters for protecting the operation of IP routers and other network components.

Also, you should enable bridging if the root access point and the gateway that supports the NNL devices are on different IP subnets. You may also need to enable bridging if your wireless end devices use terminal emulation running the NNL protocol or if you use wireless end devices that are running both IP and NNL.

## **Bridging Layer Functions**

Some of the significant functions supported at the bridging layer are explained below.

### **Network Organization**

Access points automatically configure into a self-organized network using a spanning tree topology. As devices are added to or removed from the network, the access points automatically reconfigure to maintain reliable operation. The spanning tree provides efficient, loop-free forwarding of frames through the network and allows rapid roaming of end devices.

The root access point initiates the spanning tree. The root coordinates the network and distributes common system parameters to other access points and wireless end devices. The root is elected from a group of access points that are designated as root candidates at the time of installation. The election process also occurs in the event of a root failure. You can configure your network with overlapping coverage so that the network automatically recovers from any single point of failure.

End devices can optionally participate in the spanning tree protocol by explicitly attaching to the network. As a result, operational parameters are easily distributed, unicast flooding is reduced or eliminated, and roaming hands-off logic is more robust.

### **Forwarding**

The access point maintains a forwarding database of all physical station addresses, and it knows the correct port for each address. The access point updates this database by monitoring source addresses on each port (backward learning), by receiving explicit attachment messages, and by examining messages exchanged between access points when

wireless end devices roam. The database also includes the power management status of each end device, which allows the access point to support the pending message feature of the network. The forwarding database allows the bridging software to make efficient forwarding decisions.

### **Switch Support**

Ethernet switches that do not comply with the 802.1D standard have difficulty handling wireless end devices that roam between different switched segments. The access point provides data link tunneling for switches that do not handle roaming. Using data link tunneling, frames for a given end device always appear on the root access point's switched segment, regardless of roaming, and the switch's routing tables remain stable.

### **Flooding Configurations**

When the destination address is unknown, standard LAN bridges flood frames on all ports. Most wireless end devices supported by the access point operate at lower speeds than Ethernet; therefore, indiscriminate flooding from a busy Ethernet backbone to an end device can consume a substantial portion of the available wireless bandwidth and reduce system performance. The access point allows you to set flooding control options for both unicast and multicast frames to free up bandwidth and improve system performance.

### **Pending Messages**

Wireless end devices may use power management to maintain battery life. These end devices wake up periodically to receive frames that arrived while their radio was powered down. The bridging software in the access point provides a pending message delivery service that allows frames to be held until the end device is ready to receive them.

### **Filtering Options**

The access point incorporates extensive filtering capabilities. Basic filters allow you to filter on DIX type, protocol port, socket, or SAP. Advanced filters let you create and group filters based on data patterns that you define.

## **About Secondary LANs and Designated Bridges**

There are two types of secondary LANs: one type is connected to the primary LAN via an IP tunnel the other type is connected wirelessly to the primary LAN. For help configuring IP tunnels, see **Configuring IP Tunnels** on page 94. For help configuring a wireless secondary LAN, see **Configuring WAPs** on page 115.



The access point that is responsible for bridging data between the secondary LAN and the primary LAN is called the designated bridge. In both types of secondary LANs, the designated bridge acts the same. The designated bridge must be an access point that has at least one radio set to Station mode or is the endpoint of an IP tunnel. If more than one access point meets at least one of these requirements, the access point with the highest secondary LAN bridge priority is the designated bridge.

If an access point has the highest bridge priority on the secondary LAN, but it is not in the radio coverage area of an access point on the primary LAN, it cannot become the designated bridge. In this case, an access point with a lower bridge priority that is in the radio coverage area or an access point on the primary LAN becomes the designated bridge. If two access points have the same secondary LAN bridge priority, the access point with the highest Ethernet address becomes the designated bridge. If the designated bridge goes offline, the remaining access points negotiate to determine which access point becomes the new designated bridge.

Designated bridges determine if the secondary LAN is bridging or non-bridging. By enabling the Ethernet bridging parameter on the designated bridge, all wireless traffic gets dumped raw on the secondary LAN. You should enable bridging if you have wired hosts on the secondary LAN that must communicate with a wireless device on the secondary LAN.

You should enable bridging unless the inbound path through a bridge or switch does not support roaming. Bridges and switches that adhere to the IEEE 802.1D standard support roaming. Some proprietary VLAN switches and ATM LANE bridges do not support roaming. If you disable the Ethernet bridging parameter on the designated bridge, the wireless traffic is encapsulated on the secondary LAN, which eliminates communication from secondary LAN end devices.

If you set the secondary LAN bridge priority to 0 on the designated bridge, you have a non-bridging secondary LAN; that is, bridging to the secondary LAN is automatically disabled.

## Configuring Global Parameters

Global parameters are configured on the root access point and on any other access point that is a root candidate (does not have a root priority of 0). The root access point sends these settings to all other access points on the network. You should set the same global parameters for the root access point and its backup candidates.

Any global parameters you set on the root access point will override parameters those you set in other access points.

### Configuring Global Flooding

Use global flooding to configure how the access points handle a frame with an unknown address. Access points try to forward frames to the port with the shortest path to the destination address. When the access point has not learned the direction of the shortest path, you can configure it to flood the frames in certain directions to try to locate the destination address.

To configure global flooding:

1. From the main menu, click Spanning Tree Settings. The Spanning Tree Settings screen appears, as shown in Figure 32.

The screenshot displays the 'Access Point Configuration' web interface. At the top, the Allied Telesyn logo and tagline 'Simply connecting the IP world' are on the left, and the title 'Access Point Configuration' is on the right. Below the title bar is a navigation menu with links: Logout, Save/Discard Changes, Upgrade Software, Distributed Network Upgrade, File System, and Help. The main heading is 'Spanning Tree Settings/'. On the left side, there is a sidebar menu under 'AP Configuration' with links to TCP/IP Settings, IEEE 802.11b Radio, Spanning Tree Settings (which is highlighted), Global Flooding, Global RF Parameters, Ethernet, IP Tunnels, Network Management, Security, and Maintenance. The main content area features a 'Submit Changes' button at the top left. Below it, there are several configuration fields: AP Name (text box with '21210100039'), LAN ID (Domain) (text box with '0'), Root Priority (text box with '1'), Ethernet Bridging (dropdown menu set to 'Enabled'), Secondary LAN Bridge Priority (text box with '0'), and Secondary LAN Flooding (dropdown menu set to 'Disabled').

**Figure 32** Spanning Tree Settings

- Click Global Flooding. The Global Flooding screen appears, as shown in Figure 33.

The screenshot shows the Allied Telesyn Access Point Configuration web interface. The top navigation bar includes links for Logout, Save/Discard Changes, Upgrade Software, Distributed Network Upgrade, File System, and Help. The main title is "Access Point Configuration". Below the navigation bar, the page is titled "Spanning Tree Settings/Global Flooding/". On the left side, there is a sidebar menu with the following items: AP Configuration, TCP/IP Settings, IEEE 802.11b Radio, Spanning Tree Settings, Global Flooding (selected), Global RF Parameters, Ethernet, IP Tunnels, Network Management, Security, and Maintenance. The main content area has a "Submit Changes" button at the top left. The settings for Global Flooding are as follows:

Multicast Flood Mode	Hierarchical
Multicast Outbound to Terminals	Enabled
Multicast Outbound to Secondary LANs	Set locally
Unicast Flood Mode	Disabled

**Figure 33** Global Flooding

- Configure the Global Flooding parameters. The Global Flooding Parameters are explained below.

### **Multicast Flood Mode**

Determines the flooding structure for inbound multicast frames with unknown destination addresses.

#### **Universal**

Allows any wireless end device to communicate with any other wireless end device.

#### **Hierarchical**

Allows wireless end devices to communicate with nodes on the primary LAN but not with other wireless end devices.

#### **Disabled**

Prevents flooding.

### **Multicast Outbound to Terminals**

This parameter only applies to 802.11b radios. If multicast flood mode is not disabled, this parameter specifies if outbound multicast frames with unknown destination addresses are flooded toward wireless end devices

**Multicast Outbound to Secondary LANs**

If multicast flood mode is not disabled, this parameter specifies if outbound multicast frames with unknown destination addresses are flooded toward secondary LANs.

**Enabled**

The root access point controls flooding for all access points serving as designated bridges for the secondary LANs.

**Set locally**

Designated bridges for the secondary LANs control flooding on their LANs.

**Unicast Flood Mode**

Determines the flooding structure for inbound unicast frames with unknown destination addresses.

**Universal**

Allows any wireless end device to communicate with any other wireless end device.

**Hierarchical**

Allows wireless end devices to communicate with nodes on the primary LAN but not with other wireless end devices.

**Disabled**

Prevents flooding.

**Unicast Outbound to Terminals**

If the unicast flood mode is not disabled, this parameter specifies if outbound unicast frames with unknown destination addresses are flooded toward wireless end devices. This parameter only applies to 802.11b radios.

**Unicast Outbound to Secondary LANs**

If the unicast flood mode is not disabled, this parameter specifies if outbound unicast frames with unknown destination addresses are flooded toward secondary LAN segments.

**Enabled**

The root access point controls flooding for all access points serving as designated bridges for the secondary LANs.

**Set locally**

Designated bridges for the secondary LANs control flooding on their LANs.

4. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## Configuring Global RF Parameters

Use global RF parameters to set various parameters on the access points. If you are configuring the root access point and you set the Set Globally parameter to Enabled, the value for that parameter is set globally for all access points and wireless end devices in the network. If you are configuring the root access point and you set the Set Globally parameter to Disabled or if you are not configuring the root access point, each device uses its local setting.

To configure global RF parameters:

1. From the menu, click Spanning Tree Settings. The Spanning Tree Settings screen appears, as shown in Figure 34.

**Allied Telesyn**  
Simply connecting the IP world

**Access Point Configuration**

Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File System | Help

**Spanning Tree Settings/**

**AP Configuration**

- TCP/IP Settings
- IEEE 802.11b Radio
- Spanning Tree Settings
- Global Flooding
- Global RF Parameters
- Ethernet
- IP Tunnels
- Network Management
- Security
- Maintenance

Submit Changes

AP Name	21210100039y
LAN ID (Domain)	0
Root Priority	1
Ethernet Bridging	Enabled ▼
Secondary LAN Bridge Priority	0
Secondary LAN Flooding	Disabled ▼

**Figure 34** Spanning Tree Settings

- Click Global RF Parameters. The Global RF Parameters screen appears, as shown in Figure 35.



**Figure 35** Global RF Parameters

- Configure the global RF parameters. Click the links in the Global RF Parameters menu to set more parameters. The parameters are explained below.

### **RFC1042/DIX Conversion**

Determines how the access point will handle the conversion of RFC1042/DIX frames that are received on its 802.11b ports.

#### **Enabled**

Causes frames received on an 802.11b port with a protocol type equal to a value in the "RFC1042 types to pass through" list to be forwarded without conversion. If the frame has a protocol types that is not found in the list, it will be converted to DIX format before it is forwarded.

#### **Disabled**

Causes frames received on an 802.11b port to be forwarded without conversion; that is, when a SNAP frame is received from an 802.11b radio with an OUI (Organizationally Unique Identifier) equal to 000000, it will be forwarded without conversion.

**RFC1042 Types to Pass Through**

If the RFC1042/DIX Conversion field is Enabled, this parameter specifies values for protocol types that are to be passed without conversion. The list includes the Apple Talk protocol type, value 80F3.

Values entered in this parameter represent the protocol types of frames that will be passed without conversion to DIX format.

4. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## About IP Tunnels

---

The physical boundary of a wireless network is usually defined by the presence of an IP router. Multiple independent wireless networks may exist, each with its own LAN ID, root access point, and set of wireless end devices. In this environment, an end device can only operate within the limited coverage area of its own network and cannot roam across IP subnet boundaries. However, using IP tunnel technology, end devices now can roam across subnet boundaries. This technology is designed to safely and transparently coexist with routed IP installations while supporting mobility for end devices. IP tunnels do the following:

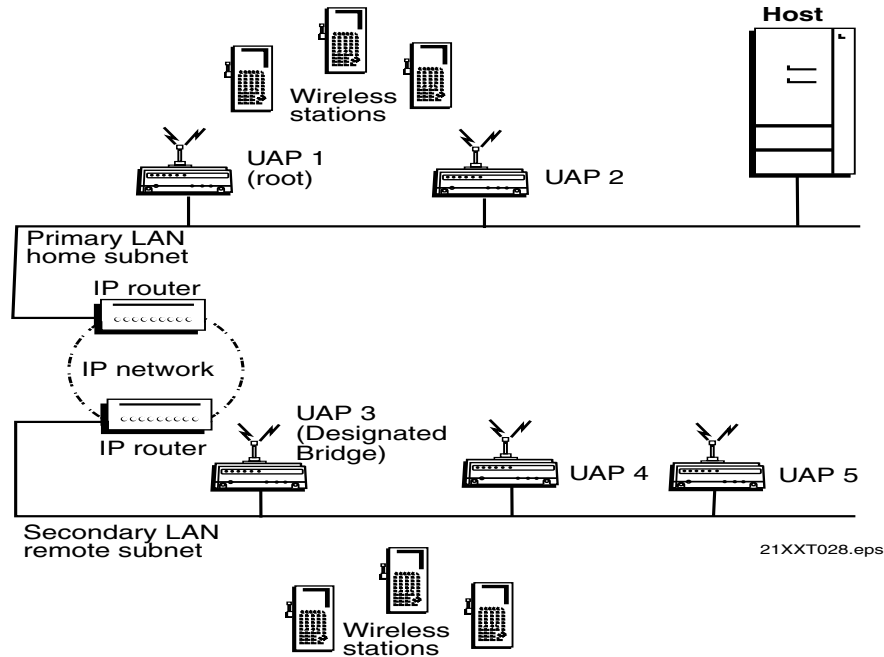
- ☐ Enables access points on different subnets to belong to the same wireless network.
- ☐ Supports transparent roaming of end devices between access points that are on different subnets without losing network connections.
- ☐ Supports end devices using both IP and other routable or nonroutable protocols.

The access point consists of a group of multiport Ethernet-to-wireless bridges. The IP tunnel port uses a standard IP protocol called Generic Routing Encapsulation (GRE) to encapsulate a frame. These encapsulated frames can use normal IP routing to pass through IP routers. Unlike the physical Ethernet and radio ports, the IP tunnel port does not have its own output connector. It is a logical port that provides IP encapsulation services for frames that must be routed to reach their destinations. Once frames are encapsulated, they are transmitted or received through a physical port.

In other words, IP tunnels use encapsulation to establish a virtual LAN segment through IP routers. The virtual LAN segment includes the home IP subnet and logically extends to include end devices attached to access points on remote IP subnets. An IP tunnel becomes a branch in the spanning tree. Access points on remote subnets can be directly connected to an IP tunnel or indirectly connected through another access point on a remote subnet.



An IP Tunnels configuration is shown in Figure 36.



**Figure 36** IP Tunnels Configuration

A non-root access point can concurrently receive hello messages on its Ethernet port, its radio port, and its IP tunnel port. However, an access point can use only one port to attach to the network. Port priorities are structured so that an Ethernet connection is always selected first and an IP tunnel connection is always selected before a radio connection.

Setting the secondary LAN bridge priority to zero disables the bridging of wireless traffic to remote IP subnets. It allows end devices that are connected to access points on a remote IP subnet to communicate with hosts on the home subnet without bridging wireless traffic to the remote IP subnet. This is always done for IP communication since the wireless traffic is always from the home subnet and not from the remote subnet. The secondary LAN bridge priority will allow you to select the bridging mode for non-IP traffic such as NNL.

### Internet Group Management Protocol (IGMP)

IGMP lets you originate multiple IP tunnels using a single IP multicast address. Note that IGMP is independent of IP; it can be used to facilitate multicast for IP or any other application.

IP routers only forward multicast packets to those subnets that have IP hosts that participate in the respective IP multicast group. An IP host uses IGMP to notify IP routers that it wants to participate in an IP multicast group. Access points can act as IP hosts and participate in an IP

multicast group by enabling IGMP and by defining a Class D IP multicast address. The Internet Assigned Numbers Authority has allocated 224.0.1.65 as an inter-access-point protocol (IAPP). You must enter this address in the IP address list in the root access point. (Note that the address list may contain other IP addresses.) and in the Multicast Address field in the other access points.

If you enable IGMP on the root access point, the root access point uses a Class D IP multicast address to send IP hello packets through IP routers to access points on other subnets. If you enable IGMP on remote IP subnets, intermediate IP routers will forward the IP hello packets to those subnets. Enabling IGMP also has these advantages:

- ☐ Causes IP hello packets to be forwarded only to those subnets that participate in the IP multicast group.
- ☐ Increases redundancy because multiple access points on a remote subnet can receive IP hello packets.

IP multicast provides an ideal way to distribute IP hello messages. Normally, you should enable IGMP and configure an IP multicast address in at least one access point on each remote IP subnet. (Some routers can provide proxy IGMP services for IP hosts.) IP multicast has the following advantages:

- ☐ The user does not have to know unicast or directed broadcast IP addresses in advance.
- ☐ IP multicast provides better built-in redundancy than IP unicast, because any access point can establish an IP tunnel.

IP hello messages are only forwarded to those IP subnets and IP hosts (such as access points) that participate in the multicast group. Directed broadcast packets are forwarded to all IP hosts on the target subnet.

## **Originating IP Tunnels**

The creation of tunnels between the root access point on the home IP subnet and access points on remote IP subnets is controlled by three operational parameters:

- ☐ Enabled/disabled IP ports. A tunnel can never be established on a disabled IP port.
- ☐ IP address list
- ☐ Secondary LAN bridge priority settings

An IP tunnel is established when an access point on a remote IP subnet attaches to the root access point through its IP tunnel port. The number of IP tunnels the root access point can originate is practically unlimited. However, the IP address list can presently contain eight entries. The size of the address list effectively limits the number of tunnels that can be created if unicast and directed broadcast IP addresses are used; however, you can use a single IP multicast address to originate a practically unlimited number of tunnels.

The IP address list can contain any combination of IP unicast, IP broadcast, or IP multicast addresses. Only one IP tunnel can be created for each IP unicast address in the list. A single IP multicast address can be used to create a practically unlimited number of tunnels to multiple remote IP subnets. A single IP directed broadcast address can be used to create a practically unlimited number of tunnels to a single remote IP subnet. (An IP directed broadcast address is typically used to specify all hosts on a single remote subnet.)

A remote IP subnet functions much like a wireless secondary LAN with these exceptions:

- ☐ Any access point can provide a wireless link to another access point. Only the root access point can originate an IP tunnel.
- ☐ A wireless link can provide a transparent bridge for both wired and wireless devices on a wireless secondary LAN. An IP tunnel only provides a transparent bridge for end devices (unless explicitly configured to provide connectivity for an NNL gateway on a remote IP subnet).

## **Establishing and Maintaining IP Tunnels**

If the IP tunnel port control is enabled, the root access point sends hello messages to each IP address in its IP address list. An access point on a remote IP subnet automatically establishes an IP tunnel if it receives an IP hello message from the root access point. An access point attached through an IP tunnel transmits hello messages on the remote subnet so that other access points on the remote subnet that do not receive IP hello messages can also attach to the network.

If IP hello messages are sent to IP unicast addresses, then some access points on a remote subnet will not receive hello messages; therefore, those access points cannot establish an IP tunnel. If bridging is disabled on the subnet, wireless traffic is forwarded to and from these access points through data link tunnels. A data link tunnel is logically concatenated with an IP tunnel so that wireless traffic can be completely isolated from the remote IP subnet.

If you need to bridge to a remote subnet, see “Configuring the Spanning Tree Parameters” earlier in this chapter.

## **IP Addressing for End Devices**

IP end devices must be assigned IP addresses that are on the home IP subnet. There are no address restrictions for non-IP end devices.

## **Using Non-IP Protocols**

Servers that use a routable network protocol such as IP or IPX may be located on any subnet; however, triangular routing can be minimized if servers are located on the home IP subnet. (Note that this is also true for standard mobile IP.) You should be able to use default flooding and bridging settings if you are using routable protocols, even if servers are located on remote IP subnets.

The NNL protocol is a simple Non-routable Network Layer protocol that is used to carry high-layer data in a local area network environment. An NNL gateway forwards NNL traffic to non-NNL hosts such as TCP/IP hosts. You can use the default flooding and bridging settings, and minimize triangular routing, if NNL gateways are located on the home subnet. If NNL gateways are located on remote subnets, you must enable outbound multicast flooding and secondary bridging.

## **Frame Forwarding**

Any data packet sent through an IP tunnel is addressed to the unicast IP address of the access point at the other end of the tunnel. An access point at the remote end of the tunnel learns the unicast IP address of the root access point by listening to IP hello packets. The root access point learns the unicast IP address of a remote access point when the access point attaches to the network.

Usually, ARP requests (which are multicast packets) that originate on the home IP subnet are forwarded outbound to all devices on the network, including through IP tunnels to remote IP subnets. If you configure the access point as an ARP server, ARP packets are only sent through the IP tunnel to the destination end device.

Unicast frames are only forwarded outbound through an IP tunnel if the destination address identifies an end device that has roamed to a remote IP subnet. Usually, wireless traffic is not bridged to remote IP subnets and traffic from a remote IP subnet is never forwarded inbound through an IP tunnel.

MAC frames originating on the home IP subnet are encapsulated in the root access point, forwarded through the IP network, unencapsulated by the access point at the remote end of the IP tunnel, and forwarded to the appropriate access point (if necessary) for delivery to the destination end device. For inbound frames, the same process is used in reverse between the access point at the remote end of an IP tunnel and the root access point.

Certain frame types are never forwarded through tunnels. Frame types that are never forwarded include IP frames used for coordinating routers and MAC frames used for coordinating bridges. Frame types that are never forwarded include:

- ☐ 802.1D bridge frames
- ☐ Proprietary VLAN switch frames
- ☐ IP frames with a broadcast or multicast Ethernet address
- ☐ IP frames with the following router protocol types and decimal values:
  - DGP (86) (Dissimilar Gateway Protocol)
  - EGP (8) (Exterior Gateway Protocol)
  - IDPR (35) (Inter-Domain Policy Routing Protocol)
  - IDRP (45) (Inter-Domain Routing Protocol)
  - IGP (9) (Interior Gateway Protocol)
  - IGRP (88)
  - MHRP (48) (Mobile Host Routing Protocol)
  - OSPFGRP (89) (Open Shortest Path First Interior Gateway Protocol)
- ☐ IP ICMP (Internet Control Message Protocol) types:
  - IPv6
  - Mobile IP
  - Router Advertisement
  - Router Selection
- ☐ IP/UDP (User Datagram Protocol) frames with the following destination protocol port numbers:
  - BGP (179) (Border Gateway Protocol)
  - RAP (38) (Route Access Protocol)
  - RIP (520) (Routing Information Protocol)
- ☐ IP/TCP frames with the following destination or source protocol port numbers:
  - BGP (179) (Border Gateway Protocol)
  - RAP (38) (Route Access Protocol)

## Outbound Frames.

Data frames are forwarded outbound through an IP tunnel if

- ☐ an end device is known to be attached to an access point on a remote IP subnet.
- ☐ the frame type is enabled in the Tunnel Filters menu.

Unicast frames are not flooded. End devices attach to the root access point, which maintains entries for these devices in its forwarding database. The database entries indicate the correct subnet for outbound forwarding.

For TCP/IP applications, IP and ARP frames must be forwarded through IP tunnels. An IP or ARP frame is only forwarded outbound if the destination address identifies an end device on the home IP subnet. If you enable the ARP server in the root access point, you can reduce the number of ARPs forwarded outbound. For help, see **Configuring the Access Point as an ARP Server** on page 58.

## Inbound Frames.

Only frame types that are enabled in the Tunnel Filters menu are forwarded, and the frames are only forwarded inbound if the source IP address belongs to the home IP subnet. Frames transmitted by servers or devices that are wired to a remote IP subnet are not forwarded through IP tunnels if the IP address does not belong to the home subnet. Only frames from wireless end devices with IP addresses belonging to the home subnet are forwarded inbound.

## Configuring IP Tunnels

In general, here are some guidelines you can use to configure IP tunnels:

- ☐ When choosing the home IP subnet, ideally you should choose the subnet that contains gateways or servers for end devices; however, these servers may be on other subnet. Note that you can create a home subnet for end devices. Fixed or variable length subnet masks can be used; subnet addressing is not required. IP addresses for end devices must belong to the home subnet.
- ☐ Identify the root candidates on the home subnet. The root access point should be an access point that does not otherwise handle a large volume of traffic.
- ☐ Configure all access points on the home subnet and remote IP subnets with the same LAN ID. If IP tunnels are not used to attach a remote subnet, then access points on that subnet should be configured with a different LAN ID.

- ❑ In the IP Tunnels screen, enable the Port Control parameter in all access points that are root candidates and designated bridge candidates.
- ❑ In the IP Tunnels screen, configure the Mode parameter in root candidates to Originate if Root. Configure the Ethernet Address table to include access points on each remote subnet. All root candidates should be configured identically.
- ❑ In the IP Tunnels screen, configure the Mode parameter in designated bridge candidates to Listen.
- ❑ In the Tunnel Filters screen, configure the filters in root candidates and in other access points that can be attached through an IP tunnel. IP tunnel filters are consistent with Ethernet filters.
- ❑ For networks using IP networking on end devices, it is recommended that you enable the ARP server capability in the access points.
- ❑ Determine if you need to enable bridging on remote subnets. For example, bridging must be enabled if an NNL gateway is attached to the remote subnet. For help, see **Configuring the Spanning Tree Parameters** on page 74. The designated bridge candidates must have permanent IP addresses and must be able to receive IP hello messages from the root access point. An access point will receive IP hello messages if the messages are sent to the unicast IP address of the access point, or to an IP-directed broadcast or IP multicast address. Note you may need to enable IGMP for IP multicast.

To configure the IP Tunnels screen:

1. From the main menu, click IP Tunnels. The IP Tunnels screen appears, as shown in Figure 37.

**Figure 37** IP Tunnels

2. Click the down arrow on the right side of the Port Control field and choose Enabled. Choose Disabled if you do not want this access point to participate in IP tunnels.
3. Click the down arrow on the right side of the Mode field and choose Originate if Root to let the access point originate the tunnel if it is functioning as the root access point for the network.
4. Click the down arrow on the right side of the IGMP field and choose Enabled or Disabled.
5. Click Submit Changes.

---

**Note**

If you enable IGMP on the root access point, you need to enter the Class D IP multicast address in the IP address list. For help, see the next procedure: **To configure the IP address list:** on page 97.

---

6. In the Multicast Address field, enter the multicast address. Unless you have your own IP multicast address, the Internet Assigned Numbers Authority has allocated 224.0.1.65 for the inter-access-point protocol (IAPP). You should use this default multicast address.



- Click **Submit Changes** to save your changes. To activate your changes, click the **Save/Discard Changes** link in the menu bar and then click **Save Changes and Reboot**. For help, see **Saving Your Configuration Changes** on page 46.

To configure the IP address list:

- From the main menu, click **IP Tunnels** and then click **IP Addresses**. The IP Addresses screen appears, as shown in Figure 38.

The screenshot shows the Allied Telesyn web interface for Access Point Configuration. The top navigation bar includes links for Logout, Save/Discard Changes, Upgrade Software, Distributed Network Upgrade, File System, and Help. Below this, the page title is 'Access Point Configuration' and the current page is 'IP Tunnels/IP Addresses/'. The left sidebar shows the 'AP Configuration' menu with sub-items: TCP/IP Settings, IEEE 802.11b Radio, Spanning Tree Settings, Ethernet, IP Tunnels, IP Addresses (selected), Tunnel Filters, Network Management, Security, and Maintenance. The main content area features a 'Submit Changes' button and a table for configuring IP addresses.

Address	Value
Address 1	0.0.0.0
Address 2	0.0.0.0
Address 3	0.0.0.0
Address 4	0.0.0.0
Address 5	0.0.0.0
Address 6	0.0.0.0
Address 7	0.0.0.0
Address 8	0.0.0.0

**Figure 38** IP Addresses

- If you enabled IGMP, enter the Class D IP multicast address. The default is 224.0.1.65.
- Enter the IP unicast addresses of the access points that can be the endpoints of IP tunnels.
- Click **Submit Changes** to save your changes. To activate your changes, click the **Save/Discard Changes** link in the menu bar and then click **Save Changes and Reboot**. For help, see **Saving Your Configuration Changes** on page 46.

## Configuring IP Tunnel Filters

You can set both Ethernet and IP tunnel filters, and you can create protocol filters for predefined protocol types. In addition, you can define arbitrary frame filters based on frame content. For help configuring Ethernet filters, see **Configuring Ethernet Filters** on page 64.

To configure IP tunnel filters:

1. From the main menu, click IP Tunnels and then click Tunnel Filters. The Tunnel Filters screen appears, as shown in Figure 39.



**Figure 39** Tunnel Filters

2. Click the down arrow on the right side of the IP Multicast field and choose Drop or Pass. This parameter specifies if the access point can receive IP multicast packets through the IP tunnel port.
3. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

### Using IP Tunnel Frame Type Filters

The IP port automatically provides some filtering for end devices. You can define permanent IP port filters to prevent unwanted frame forwarding through an IP tunnel. IP ICMP packets with the following types are forwarded:

- ☐ Echo Request
- ☐ Echo Reply
- ☐ Destination Unreachable
- ☐ Source Quench
- ☐ Redirect
- ☐ Alternate Host Address
- ☐ Time Exceeded
- ☐ Parameter Problem
- ☐ Time Stamp
- ☐ Time Stamp Reply
- ☐ Address Mask Request
- ☐ Address Mask Reply
- ☐ Trace Route

IP and ARP frames are never forwarded inbound through an IP tunnel to the home subnet unless the source IP address belongs to the home subnet. (Frames are only forwarded inbound if the source IP address in the IP or ARP packet identifies an end device that has roamed away from its home subnet.) IP and ARP frames are never forwarded outbound through an IP tunnel by the root access point unless the destination IP address belongs to the home subnet. (Frames are only forwarded outbound to end devices that have roamed away from the home subnet.) For detailed information about other frame types that are never forwarded, see the list of frame types that are never forwarded in “Frame Forwarding” earlier in this chapter.

You can set the default action and scope for general and specific frame types.

**Action**

Set the action to Pass or Drop. If you select Pass, then all frames of that type are passed. If you select Drop, then all frames of that type are dropped.

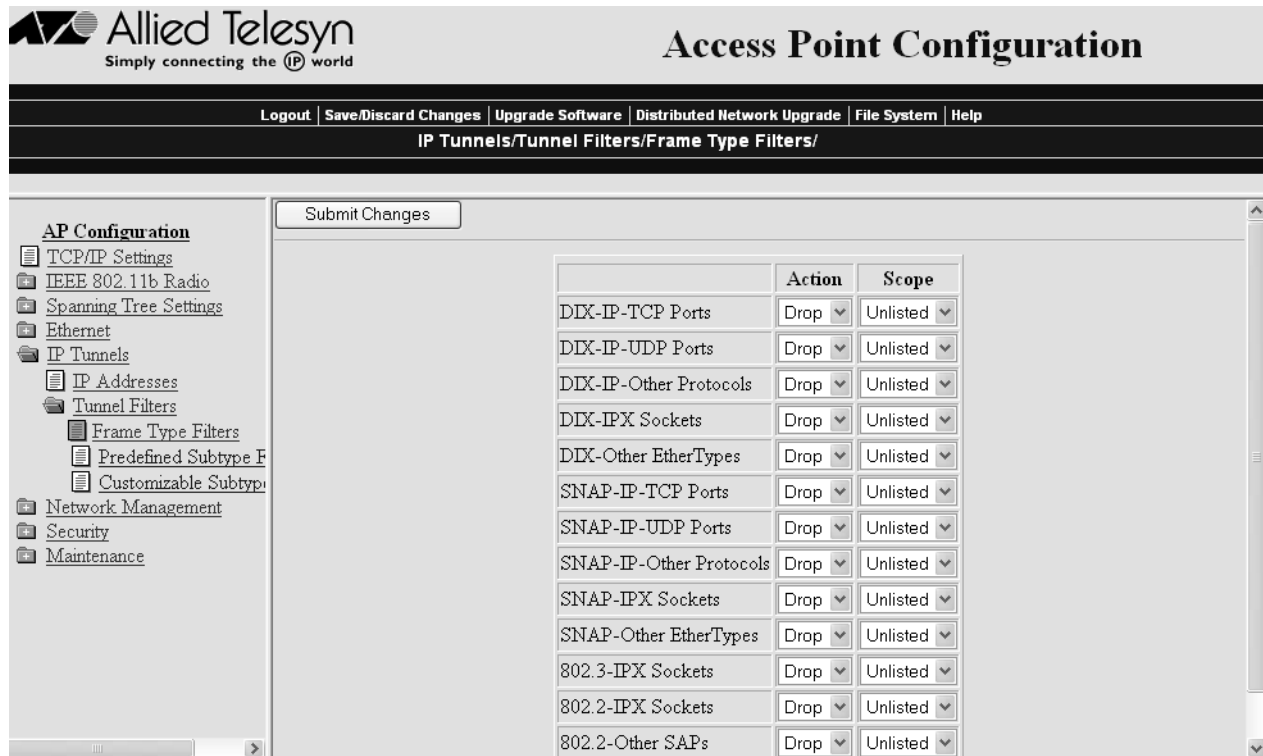
**Scope**

Set the scope to Unlisted or All. If you select All, then all frames of that type are unconditionally passed or dropped, depending on

the action you specified. If you select Unlisted, then frames are passed or dropped only if the frame type is not listed in the predefined or customizable tables.

To use IP tunnel frame type filters:

1. From the main menu, click IP Tunnels and then click Tunnel Filters.
2. Click Frame Type Filters. The Frame Type Filters screen appears, as shown in Figure 40.



**Figure 40** Frame Type Filters

3. In each frame type field, click the down arrow on the right side of the Action field and set the action to Pass or Drop.
4. In each frame type field, click the down arrow on the right side of the Scope field and set the scope to Unlisted or All.

The various frame type filters are explained below:

**DIX IP TCP Ports**

**DIX IP UDP Ports**

**SNAP IP TCP Ports**

**SNAP IP UDP Ports**

Primary Internet Protocol Suite (IP) transport protocols.

### **DIX IP Other Protocols**

### **SNAP IP Other Protocols**

IP protocols other than TCP or User Datagram Protocol (UDP).

### **DIX IPX Sockets**

Novell NetWare protocol over Ethernet II frames.

### **SNAP IPX Sockets**

Novell NetWare protocol over 802.2 SNAP frames.

### **802.3 IPX Sockets**

Novell NetWare protocol over 802.3 RAW frames.

### **DIX Other Ethernet Types**

### **SNAP Other Ethernet Types**

DIX or SNAP registered protocols other than IP or IPX.

### **802.2 IPX Sockets**

Novell running over 802.2 Logical Link Control (LLC).

### **802.2 Other SAPs**

802.2 SAPs other than IPX or SNAP.

---

#### **Note**

If you set the Scope field to Unlisted for any of the frame types, you must also configure predefined subtype filters or customizable subtype filters. For help, see **Using Predefined Subtype Filters** on page 101 or **Customizing Subtype Filters** on page 102.

---



---

#### **Note**

You cannot filter HTTP, Telnet, SNMP, and ICMP frames, because they are used for configuration and management of the access point. Additionally, you cannot filter broadcast ARP request packets if the target IP address belongs to the local access point or to an access point in the subtree rooted at the local access point.

---

5. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

### **Using Predefined Subtype Filters.**

You can configure the access point to pass or drop certain predefined frame subtypes.

To configure predefined subtype filters:

1. From the main menu, click IP Tunnels and then click Tunnel Filters.
2. Click Predefined Subtype Filters. The Predefined Subtype Filters screen appears, as shown in Figure 41.

**Allied Telesyn**  
Simply connecting the IP world

**Access Point Configuration**

Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File System | Help

IP Tunnels/Tunnel Filters/Predefined Subtype Filters/

Submit Changes

	Action	SubType	Value
DIX-ARP	Drop	DIX-EtherType	08 06
SNAP-ARP	Drop	SNAP-EtherType	08 06
802.2-IPX-RIP	Drop	802.2-IPX-Socket	04 53
802.2-IPX-SAP	Drop	802.2-IPX-Socket	04 52
NNL	Pass	DIX-EtherType	87 5b
NETBIOS	Drop	802.2-SAP	f0 f0
ICMP	Drop	DIX-IP-Protocol	00 01

**Figure 41** Predefined Subtype Filters

3. In each frame subtype field, click the down arrow on the right side of the Action field and choose Pass or Drop.
4. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

### Customizing Subtype Filters.

You can define output filters that restrict customized frame subtypes that can pass through an IP tunnel. Frames can be filtered by the DIX, 802.2, or 802.3 SNAP type, the IP protocol type, or the TCP or UDP port number. By default, the filters drop all protocol types except the NNL DIX Ethernet type (hexadecimal 875B). Filters must be configured in all root candidates and in any access point that can attach to the remote end of an IP tunnel. You define the action, subtype, and value parameters in customized filters.

**Action**

Set the action to Pass or Drop. If you select Pass, then all frames of that type are passed. If you select Drop, then all frames of that type are dropped.

**Subtype**

Selects the frame subtype you wish to filter.

**Value**

Specifies the value of the subtype. Refer to the following table for the value for a specific subtype. The value must be two hex pairs. You must enter port values as decimals; for example enter "23." for port 23. The access point displays the hexadecimal equivalent in the Value field. When a match is found between frame subtype and value, the specified action is taken.

To customize subtype filters:

1. From the main menu, click IP Tunnels and then click Tunnel Filters.
2. Click Customizable Subtype Filters. The Customizable Subtype Filters screen appears, as shown in Figure 42.

**Allied Telesyn**  
Simply connecting the IP world

**Access Point Configuration**

Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File System | Help

IP Tunnels/Tunnel Filters/Customizable Subtype Filters/

Submit Changes

	Action	SubType	Value
1	Drop	DIX-IP-TCP-Port	00 00
2	Drop	DIX-IP-TCP-Port	00 00
3	Drop	DIX-IP-TCP-Port	00 00
4	Drop	DIX-IP-TCP-Port	00 00
5	Drop	DIX-IP-TCP-Port	00 00
6	Drop	DIX-IP-TCP-Port	00 00
7	Drop	DIX-IP-TCP-Port	00 00
8	Drop	DIX-IP-TCP-Port	00 00
9	Drop	DIX-IP-TCP-Port	00 00
10	Drop	DIX-IP-TCP-Port	00 00
11	Drop	DIX-IP-TCP-Port	00 00
12	Drop	DIX-IP-TCP-Port	00 00

**AP Configuration**

- TCP/IP Settings
- IEEE 802.11b Radio
- Spanning Tree Settings
- Ethernet
- IP Tunnels
  - IP Addresses
  - Tunnel Filters
    - Frame Type Filters
    - Predefined Subtype F
    - Customizable Subtype
- Network Management
- Security
- Maintenance

**Figure 42** Customizable Subtype Filters

3. Click the down arrow on the right side of the Action field and choose Pass or Drop.
4. Click the down arrow on the right side of the SubType field and choose the customizable frame subtype.

5. Click the down arrow on the right side of the Value field and enter the two hex pair. The frame subtypes and their values are described below.

**DIX-IP-TCP-Port**

Port value in hexadecimal.

**DIX-IP-UDP-Port**

Port value in hexadecimal.

**DIX-IP-Protocol**

Protocol number in hexadecimal.

**DIX-IPX-Socket**

Socket value in hexadecimal.

**DIX-EtherType**

Specify the registered DIX type in hexadecimal.

**SNAP-IP-TCP-Port**

Port value in hexadecimal.

**SNAP-IP-UDP-Port**

Port value in hexadecimal.

**SNAP-IP-Protocol**

Port value in hexadecimal.

**SNAP-IPX-Socket**

Socket value in hexadecimal.

**SNAP-EtherType**

SNAP type in hexadecimal. To filter on both SNAP type and OUI, use advanced filters.

**802.3-IPX-Socket**

Socket value in hexadecimal.

**802.2-IPX-Socket**

Socket value in hexadecimal.

**802.2-SAP**

802.2 SAP in hexadecimal.

6. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.



## Chapter 6

# Configuring the Radio

---

This chapter explains how to configure the radios so that they work with your wireless end devices. It also provides some general guidelines to configuring point-to-point bridges and WAPs.

## About the Radios

---

The AT-WL2411 access point consists of a group of multiport Ethernet bridges. The 802.11b radio on the access point is:

- ☐ Wi-Fi Compliant
- ☐ Wireless Hops

The next sections explain how to configure the radio in your access point. If the radio is not installed in your access point, then you will not see it listed in the main menu.

## Configuring the IEEE 802.11b Radio

The IEEE 802.11b radio will communicate with other 802.11b radios that have the same

- ☐ SSID (Network Name).
- ☐ WEP keys. For help, see **Using 802.1x Security** on page 132.

To configure the 802.11b radio:

1. From the main menu, click IEEE 802.11b Radio. The IEEE 802.11b Radio screen appears, as shown in Figure 43.

The screenshot shows the Allied Telesyn Access Point Configuration web interface. The top header includes the Allied Telesyn logo and the text "Simply connecting the IP world". The main title is "Access Point Configuration". Below the title is a navigation bar with links: Logout, Save/Discard Changes, Upgrade Software, Distributed Network Upgrade, File System, and Help. The current page is titled "IEEE 802.11b Radio/". On the left side, there is a sidebar menu under "AP Configuration" with links to TCP/IP Settings, IEEE 802.11b Radio (selected), Wireless Bridging, Advanced Configuration, Spanning Tree Settings, Ethernet, IP Tunnels, Network Management, Security, and Maintenance. The main content area has a "Submit Changes" button at the top. Below it, there are four configuration fields: Port Control (set to Enabled), SSID (Network Name) (set to ATILAN), Frequency (set to Channel 03, 2422 MHz), and Data/Voice Settings (set to Data Traffic only).

**Figure 43** IEEE 802.11b Radio

2. Configure the parameters for the radio. The radio parameters are defined below.

### Port Control

Enables or disables the 802.11b port.

### SSID (Network Name)

The 802.11b radio communicates with other 802.11b radios with the same network name. Use this parameter to assign a network name to the access point, and then assign the same network

name to the wireless end devices that will connect to the access point. The network name is case-sensitive and can be no more than 32 alphanumeric characters.

### **Frequency**

The frequency is the particular frequency within the 2.4 to 2.5 GHz range that the access point uses to transmit and receive packets. The available frequencies are country-dependent and are determined by the radio. This parameter is only available if this radio is a master radio.

Configure all access points used in Spain, France, or Japan to a common frequency. For all other countries, you can configure all access points to a common frequency, or you can select up to three frequencies that are at least three channels (or 25 MHz) apart. You could select 2412 MHz, 2437 MHz, and 2462 MHz, for example.

You may want to use a single frequency to isolate the installation to part of the band; for example, use a single frequency if other DS systems or multiple microwave ovens are in use in the area.

For optimal performance of access points that are within range of each other, you should configure their frequencies to be five channels apart. For example, you could configure the access points to use channels 1, 6, and 11.

### **Data/Voice Settings**

This parameter is only available if this radio is a master radio.

Set to Data Traffic Only if the access point will transmit only data traffic.

Set to Voice Traffic Only if the access point will transmit only voice traffic. Voice 2 telephone packets will be sent with a priority setting. All other multicast/broadcast packets will be dropped.

Set to Data and Voice Traffic if the access point will transmit both data and voice traffic. MobileLAN voice 2 telephone packets will be sent in the high priority queue. Packets in the high priority queue are sent ahead of packets in the normal priority queue. No special filtering.

3. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## Worldwide Frequencies for the 802.11b Radio

Channel	FCC	ETSI	France	Japan	Israel
1	2412	2412		2412	
2	2417	2417		2417	
3	2422 (default)	2422 (default)		2422 (default)	2422 (default)
4	2427	2427		2427	
5	2432	2432		2432	
6	2437	2437		2437	
7	2442	2442		2442	
8	2447	2447		2447	
9	2452	2452		2452	
10	2457	2457	2457	2457	
11	2462	2462	2462 (default)	2462	
12		2467	2467	2467	
13		2472	2472	2472	
14				2484	

FCC countries include the United States, Canada, China, Taiwan, India, Thailand, Indonesia, Malaysia, Hong Kong, and most South American countries.

ETSI countries include all European Union countries except France. It also includes Switzerland, Iceland, Norway, Czech Republic, Slovenia, Slovakia, Turkey, Russia, and the United Arab Emirates.

Mexico and Singapore use the same channels as France.

The 802.11b channels that are allowed in a given country may change without notice. Be sure you use only those frequencies that are permissible in the given country.

## Configuring 802.11b Radio Advanced Parameters

You can configure other advanced parameters for the 802.11b radio, such as Data Rate, Medium Reservation, and Microwave Oven Robustness.

To configure other advanced parameters:

1. From the main menu, click IEEE 802.11b Radio. The IEEE 802.11b Radio screen appears, as shown in Figure 44.

The screenshot displays the Allied Telesyn web interface for Access Point Configuration. The top navigation bar includes links for Logout, Save/Discard Changes, Upgrade Software, Distributed Network Upgrade, File System, and Help. The main title is "Access Point Configuration". Below this, a sub-header reads "IEEE 802.11b Radio/".

On the left side, there is a sidebar menu titled "AP Configuration" with the following items: TCP/IP Settings, IEEE 802.11b Radio (selected), Wireless Bridging, Advanced Configuration, Spanning Tree Settings, Ethernet, IP Tunnels, Network Management, Security, and Maintenance.

The main content area features a "Submit Changes" button at the top. Below it, the configuration parameters for the IEEE 802.11b Radio are listed:

- Port Control: Enabled (dropdown menu)
- SSID (Network Name): ATILAN (text input field)
- Frequency: Channel 03, 2422 MHz (dropdown menu)
- Data/Voice Settings: Data Traffic only (dropdown menu)

**Figure 44** IEEE 802.11b Radio

- Click Advanced Configuration. The Advanced Configuration screen appears, as shown in Figure 45.

The screenshot shows the Allied Telesyn web interface for Access Point Configuration. The top navigation bar includes links for Logout, Save/Discard Changes, Upgrade Software, Distributed Network Upgrade, File System, and Help. The main title is "Access Point Configuration". Below this, the specific configuration page is "IEEE 802.11b Radio/Advanced Configuration/".

On the left sidebar, under "AP Configuration", the following links are listed: TCP/IP Settings, IEEE 802.11b Radio (selected), Wireless Bridging, Advanced Configuration, Spanning Tree Settings, Ethernet, IP Tunnels, Network Management, Security, and Maintenance.

The main configuration area has a "Submit Changes" button at the top. Below it, the following parameters are configured:

Data Rate	11 Mbits (High)
Data Rate Fallback	Enabled
Basic Rate	2 Mbits (Standard)
Medium Reservation	Disabled
Distance between APs	Large
Microwave Oven Robustness	Disabled
Network Name Security	802.11 compliant
DTIM Period	1
Load Balancing	Disabled
Medium Density Distribution	Disabled

**Figure 45** Advanced Configuration

- Configure the advanced parameters. The advanced parameters are described below:

#### **Data Rate**

Choose the rate at which the access point transmits data. In general, higher speeds mean shorter range and lower speeds mean longer range. You can set this rate to 11, 5.5, 2, or 1 Mbps.

#### **Data Rate Fallback**

Determines if you want the radio to drop to a slower data rate when it has trouble communicating with another radio. This parameter also limits your range to the Data Rate selected above.

#### **Basic Rate**

Choose the rate at which the access point transmits multicast frames. In general, higher speeds mean shorter range and lower speeds mean longer range. Do not set this rate higher than the maximum rate at which your end devices can receive multicast frames. You can set this rate to 11, 5.5, 2, or 1 Mbps. This parameter should usually be left at the default 2 Mbps.

**Medium Reservation**

Determines if you want to specify a reservation threshold. Choose Enabled to set a threshold value. If you choose Disabled, you may improve network response time in installations that primarily send very small frames or that have no hidden stations.

**Reservation Threshold**

If you enable medium reservation, you need to set a threshold value, which is the largest data packet that can be transmitted without reserving air time. Air time is normally reserved to help prevent collisions with other transmitters.

**Distance Between APs**

Controls the roaming sensitivity of your wireless end devices. This setting should match the setting on your end devices. You can use this parameter to virtually reduce the range of your access point.

If you choose Small or Medium, you do not reduce the absolute range of your radio, but you modify the collision detection mechanism to allow significant overlap of the wireless cells. Thus, you create a higher performance radio network, but you need more access points to cover an area.

**Microwave Oven Robustness**

Determines if the access point activates a modified algorithm for automatic rate fallback, which prevents the access point from falling back to 1 Mbps when trying to retransmit radio packets when 2.4 GHz interference is present.

**Network Name Security**

Determines if wireless end devices that have their SSID (Network Name) set to ANY or NULL can associate with this access point.

Choose 802.11 Compliant to allow end devices with an SSID of ANY or NULL to associate with this access point. This setting is 802.11b compliant.

Choose Network Name 'ANY' Not Allowed if you want to prevent end devices with an SSID of ANY or NULL from associating with this access point.

**DTIM Period**

Specifies the number of beacon frames to skip before including a DTIM (delivery traffic indication message) in a beacon frame. Setting a higher DTIM period may conserve battery life in a wireless end device, but it may increase response time. You can set the DTIM period to a value from 1 to 65535.

**Load Balancing**

Determines if the end devices can distribute their connections across multiple access points.

**Medium Density Distribution**

Determines if these access point parameters—Medium Reservation, Distance Between APs, Microwave Oven Robustness—are distributed to end devices that are enabled to receive them.

4. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## **Configuring a Voice Network**

Voice wireless telephone systems simplify network infrastructure and network management by combining voice and data traffic over one wireless network, leveraging 802.11b wireless LAN technology.

Voice telephones and gateways operate as adjuncts to existing wireless LANs and PBXs. The voice networks use sophisticated digital spread spectrum radio technology and have highest level of integration with enterprise telephone switching and networking systems. This provides the best voice quality possible throughout the coverage area because there are no clicks, no fading, and no dead spots.

If you are using a voice network with the access points, you need to configure the access point 802.11b port to accept voice traffic. A single 802.11b radio can support both voice and data communications. You also need to define the normal 802.11b parameters, such as SSID (Network Name) and WEP encryption.

To configure a voice network:



1. From the main menu, click IEEE 802.11b Radio. The IEEE 802.11b Radio screen appears, as shown in Figure 46.

The screenshot shows the Allied Telesyn web interface for configuring an Access Point. The header includes the Allied Telesyn logo and the title "Access Point Configuration". Below the header is a navigation bar with links: Logout, Save/Discard Changes, Upgrade Software, Distributed Network Upgrade, File System, and Help. The main content area is titled "IEEE 802.11b Radio/". On the left is a sidebar menu under "AP Configuration" with links to TCP/IP Settings, IEEE 802.11b Radio (selected), Wireless Bridging, Advanced Configuration, Spanning Tree Settings, Ethernet, IP Tunnels, Network Management, Security, and Maintenance. The main configuration area has a "Submit Changes" button at the top. Below it are four settings: Port Control (set to Enabled), SSID (Network Name) (set to ATILAN), Frequency (set to Channel 03, 2422 MHz), and Data/Voice Settings (set to Data Traffic only).

**Figure 46** IEEE 802.11b Radio

2. Click the down arrow on the right side of the Data/Voice Settings field and choose either Data and Voice Traffic or Voice Traffic only. For help, see **Configuring the IEEE 802.11b Radio** on page 106.
3. Click Submit Changes to save your changes.

4. From the IEEE 802.11b Radio menu, click Advanced Configuration.  
The Advanced Configuration screen appears, as shown in Figure 47.

**Allied Telesyn**  
Simply connecting the IP world

**Access Point Configuration**

Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File System | Help

**IEEE 802.11b Radio/Advanced Configuration/**

**AP Configuration**

- TCP/IP Settings
- IEEE 802.11b Radio
  - Wireless Bridging
  - Advanced Configuration**
  - Spanning Tree Settings
  - Ethernet
  - IP Tunnels
  - Network Management
  - Security
  - Maintenance

Submit Changes

Data Rate	11 MBits (High)
Data Rate Fallback	Enabled
Basic Rate	2 MBits (Standard)
Medium Reservation	Disabled
Distance between APs	Large
Microwave Oven Robustness	Disabled
Network Name Security	802.11 compliant
DTIM Period	1
Load Balancing	Disabled
Medium Density Distribution	Disabled

**Figure 47** Advanced Configuration

5. Configure these advanced parameters:

Enable the Data Rate Fallback parameter.

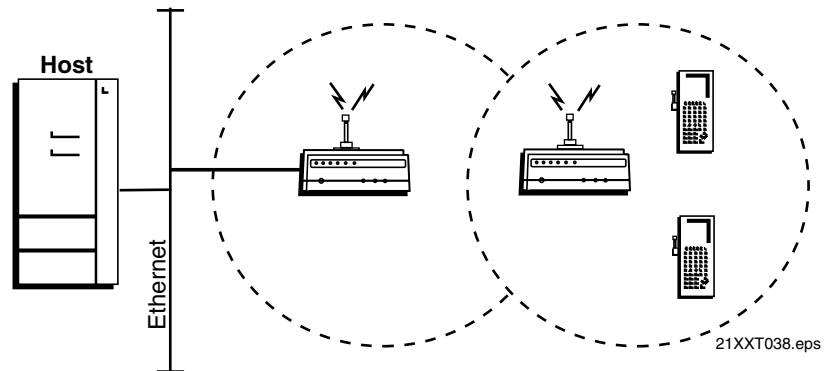
If you are using a 2 Mbps voice 2 telephone, set the Basic Rate to 2 Mbps.

If you are using a 1 Mbps voice 2 telephone, set the Basic Rate to 1 Mbps.

6. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## Configuring WAPs

In a wireless network environment, you may have WAPs, which send data from wireless end devices to wired access points. This data is sent via a wireless hop. Wireless hops are formed when data from wireless end devices move from one access point, such as a WAP, to another access point through the radio ports. Figure 48 is an example of a wireless hop that is formed between a WAP and a wired access point.



**Figure 48** WAP

It is recommended that you install no more than two WAPs for each wired access point.

Before you can create wireless hops, both the WAP and the wired access point must be on the same IP subnet. Also, the radios in both the WAP and the wired access point must be communicating with each other. For help, see how to configure the radio earlier in this chapter.

A WAP can have one or two radios installed. To create wireless hops, at least one radio in the wired access point must be configured as a master and at least one radio in the WAP must be configured as a station. If you have two radios in the WAP, one radio must be configured as a master and the other as a station. The master radio in the wired access point must have the Wireless Hops parameter enabled so that it honors connections from station radios. The master radio transmits hello packets, which allow the WAPs to attach to the spanning tree in the same way that wired access points do.

To configure the master radio (in the wired access point):

1. From the main menu, click the link corresponding to the radio that you are configuring.

2. Click Wireless Bridging. The Wireless Bridging screen appears, as shown in Figure 49.

The screenshot shows the Allied Telesyn web interface for Access Point Configuration. The top navigation bar includes links for Logout, Save/Discard Changes, Upgrade Software, Distributed Network Upgrade, File System, and Help. The current page is titled "IEEE 802.11b Radio/Wireless Bridging/". On the left, a sidebar lists various configuration options under "AP Configuration", with "Wireless Bridging" selected. The main configuration area contains a "Submit Changes" button and two dropdown menus: "Node Type" set to "Master" and "Wireless Hops" set to "Disabled".

**Figure 49** Wireless Bridging Screen - Master

3. Click the down arrow on the right side of the Node Type field and choose Master and then click Submit Changes. Your changes are saved and the Wireless Hops parameter appears.
4. Click the down arrow on the right side of the Wireless Hops field and choose Enabled and then click Submit Changes. Your changes are saved and the Hello Period parameter appears.
5. Click the down arrow on the right side of the Hello Period field and choose a hello period of 1, 2, or 3 seconds.
6. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

To configure the station radio (in the WAP):

1. From the main menu, click the link corresponding to the radio that you are configuring.

1. Click Wireless Bridging. The Wireless Bridging screen appears, as shown in Figure 50.

The screenshot displays the Allied Telesyn web interface for Access Point Configuration. The top header includes the Allied Telesyn logo and the tagline 'Simply connecting the IP world'. Below this is a navigation bar with links: Logout, Save/Discard Changes, Upgrade Software, Distributed Network Upgrade, File System, and Help. The main title is 'Access Point Configuration'. Below the title is a sub-header 'IEEE 802.11b Radio/Wireless Bridging/'. The left sidebar shows a tree view of configuration options: AP Configuration (expanded), TCP/IP Settings, IEEE 802.11b Radio, Wireless Bridging (selected), Advanced Configuration, Spanning Tree Settings, Ethernet, IP Tunnels, Network Management, Security, and Maintenance. The main content area has a 'Submit Changes' button at the top. Below it are two dropdown menus: 'Node Type' set to 'Station' and 'Wireless Hops' set to 'Disabled'.

**Figure 50** Wireless Bridging Screen - Station

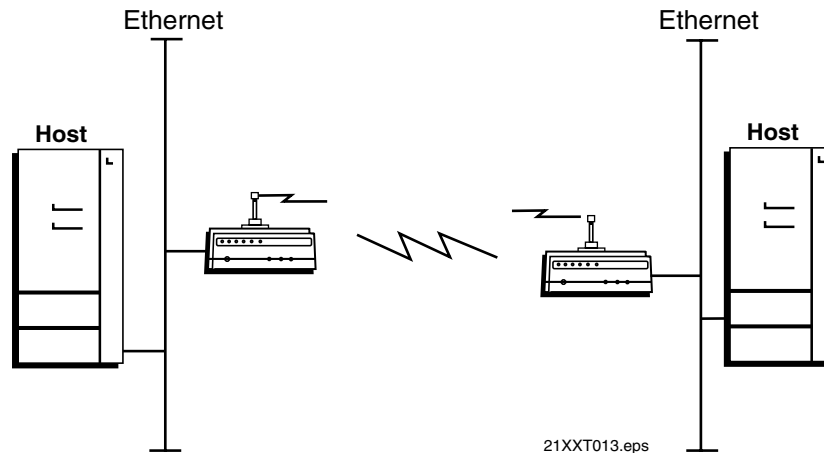
2. Click the down arrow on the right side of the Node Type field and choose Station. Wireless hops are automatically disabled.
3. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## Configuring Point-to-Point Bridges

In your environment, you may have point-to-point bridges, which send data from wireless end devices on a secondary LAN to a primary LAN. This data is sent via a wireless hop. Wireless hops are formed when data from wireless end devices move from one access point to another access point through the radio ports.

These access points can be acting simultaneously as access points and bridges or they can be acting as a bridge that is communicating to other access points. If these access points are acting as access points and bridges and if they connect 802.11b networks, each access point must contain two of the same radios. If they connect 902 MHz networks or if they are simply acting as a bridge, each access point only needs one radio.

Figure 51 illustrates a point-to-point bridge configuration.



**Figure 51** Point-to-Point Bridging

### Note

Before you can create wireless hops, the radios in the access points must be communicating with each other.

To create wireless hops, one radio in the point-to-point bridge on the primary LAN must be configured as a master and one radio in the bridge on the secondary LAN must be configured as a station. If you have two radios in the bridge, one radio must be configured as a master and the other as a station. The master radio in the bridge on the primary LAN must have the Wireless Hops parameter enabled so that it honors connections from station radios. The master radio transmits hello packets, which allow the bridge on the secondary LAN to attach to the spanning tree in the same way that wired access points do.

You need to set the root priority of the master radio to a number that is greater than the root priority of the station radio. The devices will not form a point-to-point bridge if the master radio has a lower root priority than the station radio. On the master radio, you should also set the Secondary LAN Bridge Priority parameter to 0 and the Secondary LAN Flooding parameter to disabled. On the station radio, you should set bridge priority parameter to a number other than 0 and the flooding parameter to enabled.

You may also need to adjust the flooding parameters. Follow these recommendations when configuring the flooding parameters for a point-to-point bridge:

- ☐ If there are no wireless end devices on the secondary LAN, the access point on the secondary LAN can use the default flooding settings.
- ☐ If there are wireless end devices on the secondary LAN, the access point on the secondary LAN should have its Secondary LAN Flooding parameter enabled. Also, the Secondary LAN Bridge Priority parameter must be non-zero.
- ☐ If there are wireless end devices on the secondary LAN and the end devices communicate with end devices on another secondary LAN, the root access point should have its Multicast Flood Mode parameter set to Universal.

To configure the master radio (in the point-to-point bridge on the primary LAN):

1. From the main menu, click the link corresponding to the radio that you are configuring.

2. Click Wireless Bridging. The Wireless Bridging screen appears, as shown in Figure 52.

The screenshot shows the Allied Telesyn Access Point Configuration web interface. The top navigation bar includes links for Logout, Save/Discard Changes, Upgrade Software, Distributed Network Upgrade, File System, and Help. The main title is "Access Point Configuration". Below the title, the current page is "IEEE 802.11b Radio/Wireless Bridging/". On the left, a sidebar menu lists various configuration options: AP Configuration, TCP/IP Settings, IEEE 802.11b Radio, Wireless Bridging (selected), Advanced Configuration, Spanning Tree Settings, Ethernet, IP Tunnels, Network Management, Security, and Maintenance. The main content area has a "Submit Changes" button at the top. Below it, there are two dropdown menus: "Node Type" set to "Master" and "Wireless Hops" set to "Disabled".

**Figure 52** Wireless Bridging

3. Click the down arrow on the right side of the Node Type field and choose Master and then click Submit Changes. Your changes are saved and the Wireless Hops parameter appears.
4. Click the down arrow on the right side of the Wireless Hops field and choose Enabled and then click Submit Changes. Your changes are saved and the Hello Period parameter appears.
5. Click the down arrow on the right side of the Hello Period field and choose a hello period of 1, 2, or 3 seconds and then click Submit Changes. Your changes are saved.



- From the main menu, click Spanning Tree Settings. The Spanning Tree Settings screen appears, as shown in Figure 53.

**Allied Telesyn**  
Simply connecting the IP world

**Access Point Configuration**

Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File System | Help

**Spanning Tree Settings/**

**AP Configuration**

- TCP/IP Settings
- IEEE 802.11b Radio
- Spanning Tree Settings
- Global Flooding
- Global RF Parameters
- Ethernet
- IP Tunnels
- Network Management
- Security
- Maintenance

Submit Changes

AP Name	21210100039y
LAN ID (Domain)	0
Root Priority	1
Ethernet Bridging	Enabled
Secondary LAN Bridge Priority	0
Secondary LAN Flooding	Disabled

**Figure 53** Spanning Tree Settings

- In the Root Priority field, enter a number other than 0.
- In the Secondary LAN Bridge Priority field, enter 0.
- Click the down arrow on the right side of the Secondary LAN Flooding field and choose Disabled.
- Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

To configure the station radio (in the point-to-point bridge on the secondary LAN):

- From the main menu, click the link corresponding to the radio that you are configuring.

2. Click Wireless Bridging. The Wireless Bridging screen appears, as shown in Figure 54.

The screenshot displays the Allied Telesyn web interface for Access Point Configuration. The top navigation bar includes links for Logout, Save/Discard Changes, Upgrade Software, Distributed Network Upgrade, File System, and Help. The main title is "Access Point Configuration". Below this, a sub-header reads "IEEE 802.11b Radio/Wireless Bridging/". On the left, a sidebar menu lists various configuration options: AP Configuration, TCP/IP Settings, IEEE 802.11b Radio, Wireless Bridging (selected), Advanced Configuration, Spanning Tree Settings, Ethernet, IP Tunnels, Network Management, Security, and Maintenance. The main content area features a "Submit Changes" button at the top. Below it, there are two dropdown menus: "Node Type" set to "Master" and "Wireless Hops" set to "Disabled".

**Figure 54** Wireless Bridging

3. Click the down arrow on the right side of the Node Type field and choose Station. Wireless hops are automatically disabled. Click Submit changes to save your changes.

4. From the main menu, click Spanning Tree Settings. The Spanning Tree Settings screen appears, as shown in Figure 55.

**Allied Telesyn**  
Simply connecting the IP world

**Access Point Configuration**

Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File System | Help

**Spanning Tree Settings/**

**AP Configuration**

- TCP/IP Settings
- IEEE 802.11b Radio
- Spanning Tree Settings**
- Global Flooding
- Global RF Parameters
- Ethernet
- IP Tunnels
- Network Management
- Security
- Maintenance

Submit Changes

AP Name	21210100039y
LAN ID (Domain)	0
Root Priority	1
Ethernet Bridging	Enabled ▾
Secondary LAN Bridge Priority	0
Secondary LAN Flooding	Disabled ▾

**Figure 55** Spanning Tree Settings

5. In the Root Priority field, enter 0 or another number lower than the root priority that is set in the master radio in the access point on the primary LAN.
6. In the Secondary LAN Bridge Priority field, enter a number higher than the bridge priority that is set in the master radio in the access point on the primary LAN.
7. Click the down arrow on the right side of the Secondary LAN Flooding field and choose Enabled.
8. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## Chapter 7

# Configuring Security

---

This chapter explains how to use features that are available on the access point to ensure that you have a secure wireless network.

### About Security

---

There are several levels of security that you can implement in the access points.

- ☐ Enable/disable access methods.
- ☐ Change the default logins for users who need to be able to configure and manage the access point.

Or, use a password server (external or internal to the access point) to create a list of authorized user names and passwords. Typically, this password server is a RADIUS server.

- ☐ (802.11b/802.11a) Configure static WEP keys. You can configure up to four different WEP keys on the access point and most wireless end devices. You should periodically change which WEP key these devices use to transmit data.
- ☐ Use an 802.1x authentication server (typically a RADIUS server external to the access point) with EAP-TLS or EAP-TTLS if you want to implement the 802.1x standard and automatically generated, periodically rotating WEP keys.

These security levels are described in this chapter.

## Enabling Access Methods

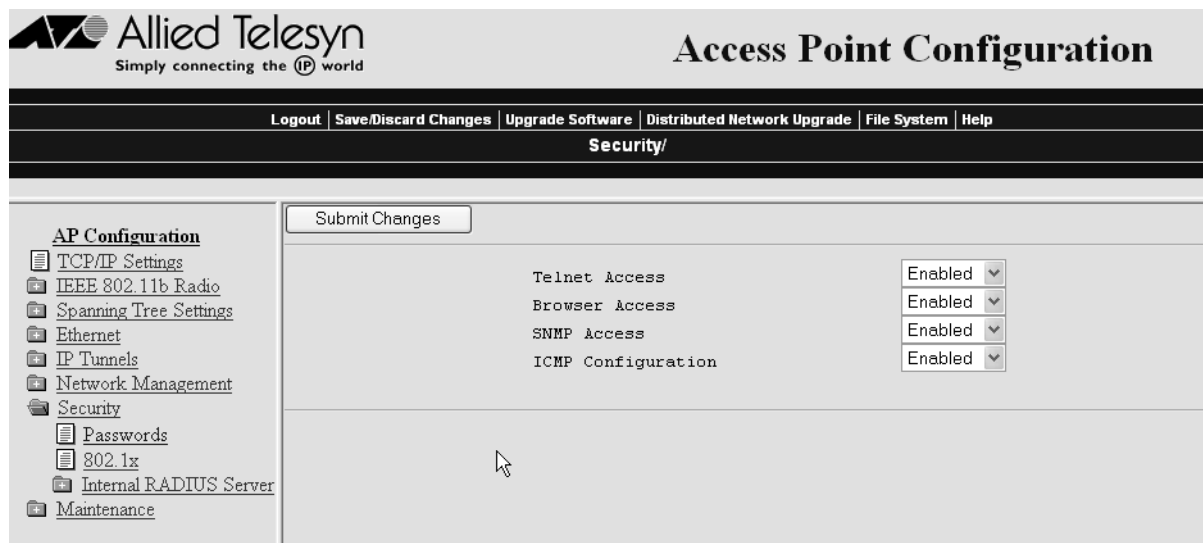
There are four access methods that you can enable or disable depending on how you want users to be able to configure or manage the access points:

- ☐ a Web browser interface
- ☐ a Telnet session
- ☐ an SNMP management station
- ☐ the MobileLAN access Utility

The default is that all access methods are enabled. You may want to disable any of these methods to prevent access by an unauthorized method.

To enable or disable access methods:

1. From the main menu, click Security. The Security screen appears, as shown in Figure 56.



**Figure 56** Security

2. Enable or disable the access methods that users can use to connect to the access point. The security parameters are explained below.

### Telnet Access

Determines if users can use a Telnet session (or a communications program) to configure or manage this access point.

**Browser Access**

Determines if users can use a Web browser to configure or manage this access point.

**SNMP Access**

Determines if users can use an SNMP management station to configure or manage this access point.

**ICMP Configuration**

Determines if users can use the Allied Telesyn access utility to set the IP address or restore factory defaults on this access point.

3. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## Setting Up Logins

---

To ensure login security for configuring or maintaining the access points, you should either use a password server (typically a RADIUS server) or immediately change the default user name and password.

To use the RADIUS password server, you must have the following:

- ☐ a password server (typically a RADIUS server) on the network that contains the user name/password database.

Or, the access point has an internal RADIUS password server that you can use to authenticate the end devices (typically PCs). For help, see **Configuring the Internal RADIUS Server** on page 130.

- ☐ an access point, which is the RADIUS client, on the network.

If you enable RADIUS authorization, a user must enter a user name and password, which is sent through the access point to the RADIUS server. The server compares the user name and password to its list of authorized user names and passwords. If a match is found, the server returns an access-accept packet and the user is logged into the access point with read/write privileges.

If no RADIUS server (#1 or #2) is available when the user attempts a login, the Service password is checked. If the user name and password do not match the Service Password, the login fails.

---

**Note**

Each time the service password login attempt fails, the process may take up to eight seconds.

---

If you do not want to use RADIUS authorization, you should change the default login user name and password. You may also want to change the read only password.

To set up logins:

1. From the main menu, click Security and then click Passwords. The Passwords screen appears, as shown in Figure 57.

Access Point Configuration

Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File System | Help

Security/Passwords/

Submit Changes

**AP Configuration**

- TCP/IP Settings
- IEEE 802.11b Radio
- Spanning Tree Settings
- Ethernet
- IP Tunnels
- Network Management
- Security
- Passwords
- 802.1x
- Internal RADIUS Server
- Maintenance

RADIUS Authorization: Disabled

User Name: [password field]

Password: [password field]

Read Only Password: [password field]

Service Password: Enabled

**Figure 57** Passwords

2. Enable or disable Radius Authorization.
3. Configure the parameters, as described below.

### **RADIUS Authorization**

Determines if you are using a RADIUS security server to authenticate devices that can communicate with this access point.

### **RADIUS Server #1 IP Address**

Enter the IP address of the RADIUS server that you want to use to authenticate user logins.

### **RADIUS Server #1 Secret Key**

Enter the shared secret key for the RADIUS server. You can enter the key from 1 to 32 characters in ASCII or in hexadecimal. To enter a hexadecimal key, it must start with 0x. For example, enter the ASCII key as ABCDE; enter the same hexadecimal key as 0x4142434445.

### **RADIUS Server #2 IP Address**

Enter the IP address of the backup RADIUS server that you want to use to authenticate user logins if RADIUS server #1 is unavailable.



**RADIUS Server #2 Secret Key**

Enter the shared secret key for the backup RADIUS server. You can enter the key from 1 to 32 characters in ASCII or in hexadecimal. To enter a hexadecimal key, it must start with 0x. For example, enter the ASCII key as ABCDE; enter the same hexadecimal key as 0x4142434445.

**User Name**

If RADIUS authorization is disabled, you can specify the user name to use to login to the access point. This parameter can be from 0 to 16 characters long.

**Password**

If RADIUS authorization is disabled, you can specify the password to use to log into the access point. This password gives the user read and write access to the access point configuration. This parameter can be from 0 to 16 characters long.

**Read Only Password**

If RADIUS authorization is disabled, you can specify the password to use to log into the access point. This password gives the user read-only access to the access point. This user is able to view the configuration and execute diagnostics, but cannot perform any tasks that affect the operation of the access point, such as changing configuration options, rebooting, or downloading software.

To disable this password, delete it.

**Service Password**

Determines if a user can use the service password to connect to this access point. Gives read-only access to the access point. It is recommended that you do not disable the service password. Enabling this password may help Technical Support help you with your installation.

4. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

Once the changes are activated, you must enter these new values when you use a Web browser to connect to this access point. This table explains the Password parameters.

## Configuring the Internal RADIUS Server

The access point has an internal RADIUS password server you can use to authorize user name and password logins. By using this password server you do not need to buy a separate server to authorize logins, but you are limited to 70 users.

### Note

Currently, you cannot use the internal RADIUS server as an 802.1x authentication server.

To configure the internal RADIUS server:

1. From the main menu, click Security and then click Internal RADIUS Server. The Internal RADIUS Server screen appears as shown in Figure 58.

The screenshot displays the 'Access Point Configuration' web interface for Allied Telesyn. The top navigation bar includes links for Logout, Save/Discard Changes, Upgrade Software, Distributed Network Upgrade, File System, and Help. The main title is 'Access Point Configuration'. Below the navigation bar, the page is titled 'Security/Internal RADIUS Server/'. On the left side, there is a tree menu under 'AP Configuration' with options: TCP/IP Settings, IEEE 802.11b Radio, Spanning Tree Settings, Ethernet, IP Tunnels, Network Management, Security (expanded), Passwords, 802.1x, Internal RADIUS Server (selected), Access Point Login D, and Maintenance. The main content area has a 'Submit Changes' button at the top. Below it, there are two fields: 'Server' with a dropdown menu set to 'Enabled', and 'Secret Key' with an empty text input field.

**Figure 58** Internal RADIUS Server

2. If Server is disabled, click the down arrow on the right side of the Server field and then choose Enabled. Click Submit Changes.
3. In the Secret Key field, enter the key from 1 to 32 characters in ASCII or in hexadecimal. To enter a hexadecimal key, it must start with 0x.
4. Click Submit Changes.

- From the Security menu, click Internal RADIUS Server and then click Access Point Login Database. The Access Point Login Database screen appears as shown in Figure 59.

	User Name	Password
User 1		
User 2		
User 3		
User 4		
User 5		
User 6		
User 7		
User 8		
User 9		
User 10		
User 11		
User 12		

**Figure 59** Access Point Login Database

- In each User Name and Password field, enter a user name and password of all the users who can log into this access point with read/write privileges.
- Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## Using 802.1x Security

---

802.1x security increases security between the access points and the wireless end devices by using an 802.1x authentication server (typically a RADIUS server) to authenticate each device's initial connection and by using rotating WEP keys.

To use 802.1x, you must have the following:

- ☐ an 802.1x authentication server (typically a RADIUS server) on the network.
- ☐ an authenticator (typically an access point) on the network
- ☐ supplicant functionality on the wireless end devices.

Currently, Windows XP devices are shipping with the supplicant functionality (using the EAP-TLS authentication method) in the operating system and NDIS 5.1 radio drivers. CE.NET will also have the same support. Multiple vendors are working on comparable functionality on other operating systems. For more information on the availability of supplicants, contact your local Allied Telesyn representative.

When a wireless end device starts communicating with a wireless network that has implemented the 802.1x security standard, the authentication process involves two steps: server side authentication and client side authentication.

For server side authentication, the 802.1x authentication server sends a certificate through the authenticator to the supplicant. The supplicant verifies that the server name is what it expects and that it can unencrypt the certificate. If the server passes, then it performs client side authentication. That is, it presents its credentials to the server for verification in one of these ways:

- ☐ If the supplicant is using the EAP-TLS authentication method, it sends a certificate through the authenticator to the 802.1x authentication server. The server verifies the device's credentials. If the credentials are accepted, the device can communicate through the access point to the network.
- ☐ If the supplicant is using the EAP-TTLS authentication method, it sends a user name and password through the authenticator to the 802.1x authentication server. The server compares the login to its list of authorized logins. If a match is found, the device can communicate through the access point to the network.

When the authentication process is complete, the end device receives the current WEP key from the access point. This WEP key is automatically generated and periodically rotated to provide a more secure network.

### Note

Currently, you cannot use this 802.1x authentication over wireless hops.

## Note

Since 802.1x authentication uses rotating WEP keys that are automatically generated, you do not configure IEEE 802.11b Radio WEP or IEEE 802.11a Radio WEP. You only configure these parameters if you are using static WEP keys.

To configure 802.1x security:

1. From the main menu, click Security and then click 802.1x. The 802.1x screen appears as shown in Figure 60.

Allied Telesyn Simply connecting the IP world	<h1>Access Point Configuration</h1>																
<a href="#">Logout</a>   <a href="#">Save/Discard Changes</a>   <a href="#">Upgrade Software</a>   <a href="#">Distributed Network Upgrade</a>   <a href="#">File System</a>   <a href="#">Help</a>																	
<b>Security/802.1x/</b>																	
<p><b>AP Configuration</b></p> <ul style="list-style-type: none"> <li>TCP/IP Settings</li> <li>IEEE 802.11b Radio</li> <li>Spanning Tree Settings</li> <li>Ethernet</li> <li>IP Tunnels</li> <li>Network Management</li> <li>Security             <ul style="list-style-type: none"> <li>Passwords</li> <li>802.1x</li> <li>Internal RADIUS Server</li> </ul> </li> <li>Maintenance</li> </ul>	<div align="center">Submit Changes</div> <hr/> <table> <tr> <td>802.1x Authentication</td> <td>Enabled ▼</td> </tr> <tr> <td>IAPP Security Context Hand Off</td> <td>Disabled ▼</td> </tr> <tr> <td>IAPP Secret Key</td> <td>XXXXXXXXXXXXXXXXXXXXX</td> </tr> <tr> <td>Key Rotation Period (Minutes)</td> <td>5</td> </tr> <tr> <td>RADIUS Server #1 IP Address</td> <td>0.0.0.0</td> </tr> <tr> <td>RADIUS Server #1 Secret Key</td> <td></td> </tr> <tr> <td>RADIUS Server #2 IP Address</td> <td>0.0.0.0</td> </tr> <tr> <td>RADIUS Server #2 Secret Key</td> <td></td> </tr> </table>	802.1x Authentication	Enabled ▼	IAPP Security Context Hand Off	Disabled ▼	IAPP Secret Key	XXXXXXXXXXXXXXXXXXXXX	Key Rotation Period (Minutes)	5	RADIUS Server #1 IP Address	0.0.0.0	RADIUS Server #1 Secret Key		RADIUS Server #2 IP Address	0.0.0.0	RADIUS Server #2 Secret Key	
802.1x Authentication	Enabled ▼																
IAPP Security Context Hand Off	Disabled ▼																
IAPP Secret Key	XXXXXXXXXXXXXXXXXXXXX																
Key Rotation Period (Minutes)	5																
RADIUS Server #1 IP Address	0.0.0.0																
RADIUS Server #1 Secret Key																	
RADIUS Server #2 IP Address	0.0.0.0																
RADIUS Server #2 Secret Key																	

### Figure 60 802.1x

2. If 802.1x Authentication is disabled, click the down arrow on the right side of the 802.1x Authentication field and then choose Enabled. Click Submit Changes.

3. Configure the parameters for 802.1x authentication. The 802.1x parameters are explained below.

**802.1x Authentication**

Determines if this access point uses 802.1x authentication.

**IAPP Security Context Hand Off**

Enable this feature to use IAPP (Inter Access Point protocol) for security context handoffs. This feature uses the advantages of the spanning tree for faster roaming. Devices do not have to perform a full reauthentication each time they roam between access points.

Disable this feature if you want to use the 802.1x standard for reauthentication or if the supplicant functionality that is implemented on the device does not support it.

**IAPP Secret Key**

Enter a key that the access points use to encrypt and sign security context exchanges. This key must be the same in all access points and can contain from 1 to 32 characters. It is recommended that this key contain at least 16 characters. You can enter the key in ASCII or in hexadecimal. To enter a hexadecimal key, it must start with 0x. For example, enter the ASCII key as ABCDE; enter the same hexadecimal key as 0x4142434445.

**Key Rotation Period**

Enter how often (in seconds) you want the access point to generate a new WEP key to use in the wireless network.

**RADIUS Server #1 IP Address**

Enter the IP address of the RADIUS server that you want to use to perform the authentication.

**RADIUS Server #1 Secret Key**

Enter the shared secret key for the RADIUS server. You can enter the key from 1 to 32 characters in ASCII or in hexadecimal. To enter a hexadecimal key, it must start with 0x. For example, enter the ASCII key as ABCDE; enter the same hexadecimal key as 0x4142434445.

**RADIUS Server #2 IP Address**

Enter the IP address of the backup RADIUS server that you want to perform the authentication if RADIUS server #1 is unavailable.

**RADIUS Server #2 Secret Key**

Enter the shared secret key for the backup RADIUS server. You can enter the key from 1 to 32 characters in ASCII or in hexadecimal.

To enter a hexadecimal key, it must start with 0x. For example, enter the ASCII key as ABCDE; enter the same hexadecimal key as 0x4142434445.

4. Click Submit Changes to save your changes. To activate your changes, click the Save/Discard Changes link in the menu bar and then click Save Changes and Reboot. For help, see **Saving Your Configuration Changes** on page 46.

## Chapter 8

# Access Point Maintenance

---

This chapter explains how to monitor the activity on the access point, how to restore the factory default settings, and how to upgrade the firmware.

## Monitoring the Access Point

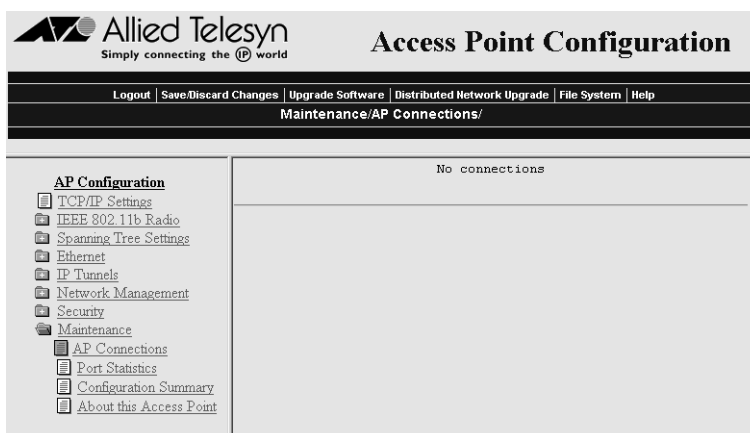
---

Using a Web browser session, you can view different parameters configured for the AT-WL2411 access point, including port statistics, connections, and a configuration summary. The information on these screens may be needed when you call Allied Telesyn Technical Support.

### Viewing Access Point Connections

The AP Connections screen shows information about the devices in the spanning subtree. To view the AP Connections screen:

1. Click Maintenance. The read-only AP Connections screen appears, as shown in Figure 61.



**Figure 61** AP Connections Screen

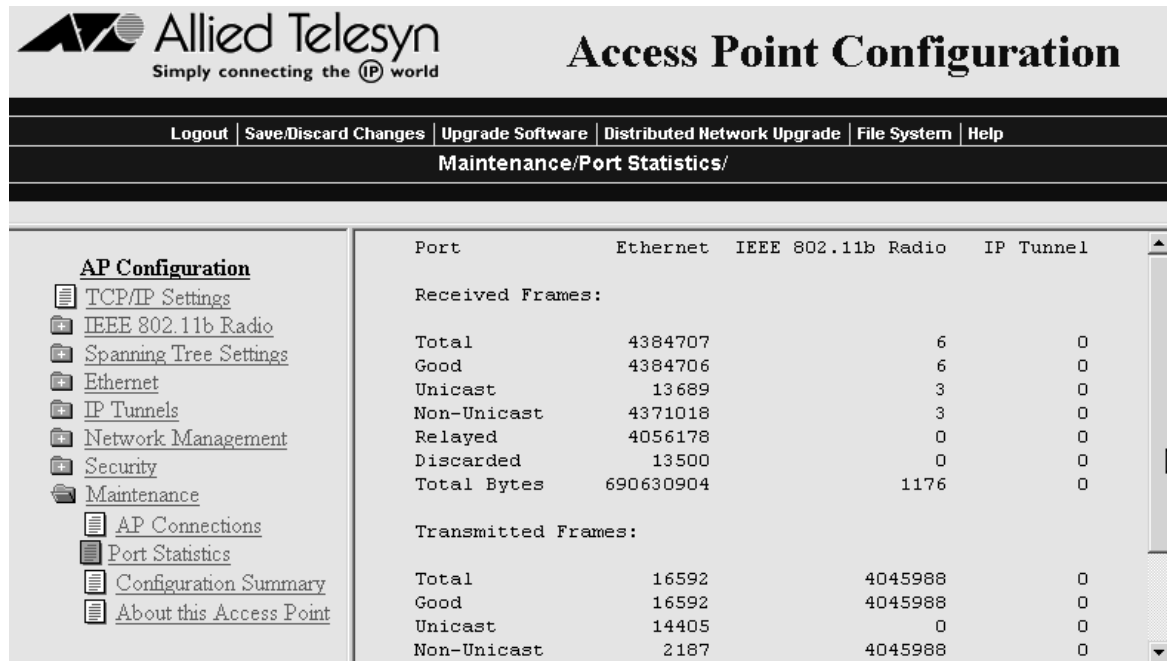


## Viewing Port Statistics

The Port Statistics screen shows the total number of frames and bytes that the access point has transmitted and received since it was last booted.

To view port statistics, do the following:

1. Click Maintenance. The read-only Port Statistics screen appears, as shown in Figure 62.



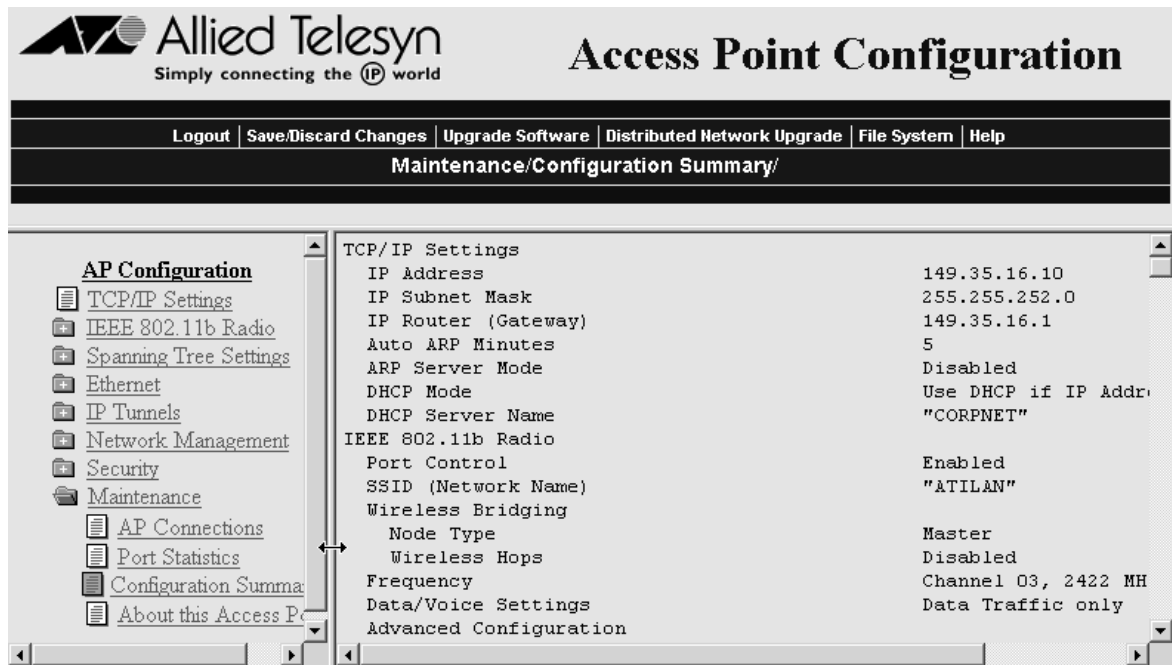
**Figure 62** Port Statistics Screen

## Viewing the Configuration Summary

The Configuration Summary summarizes the major configuration settings and installed hardware for the access point.

To view the configuration summary, do the following:

1. Click Maintenance.
2. Click Configuration Summary. The read-only Configuration Summary screen appears listing each parameter in the access point and its current configuration, as shown in Figure 63.



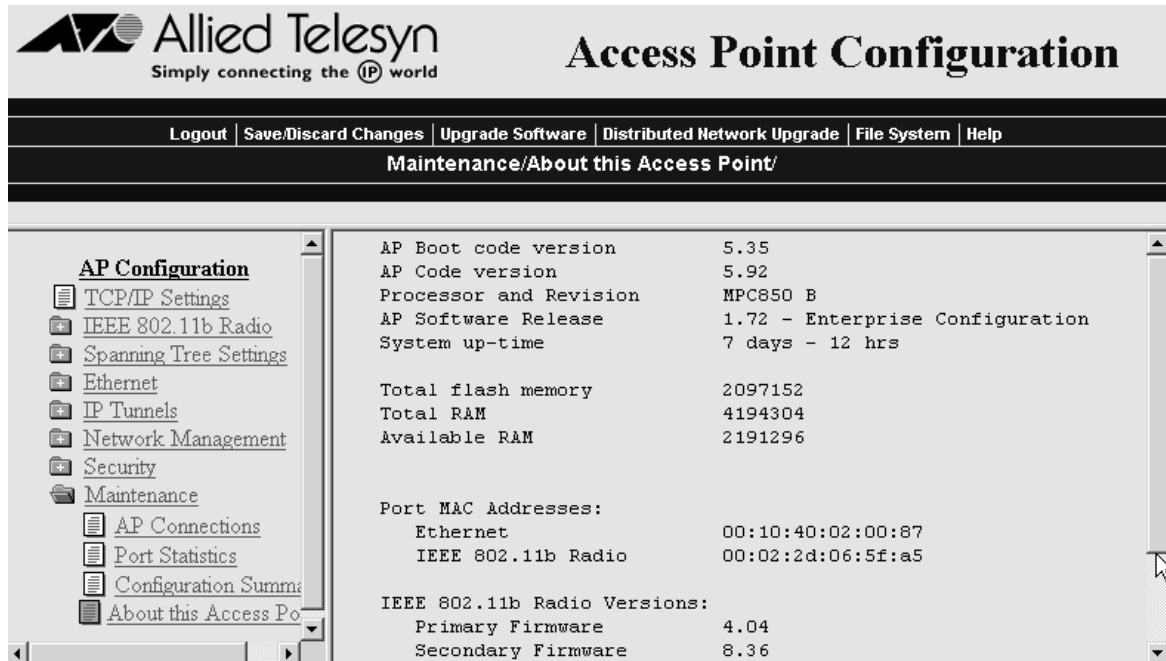
**Figure 63** Configuration Summary Screen

## Viewing Information About the Access Point

About this Access Point shows the firmware version, radio versions, and MAC addresses.

To view About this Access Point, do the following:

1. Click Maintenance.
2. Click About this Access Point. The read-only About this Access Point screen appears, as shown in Figure 64.

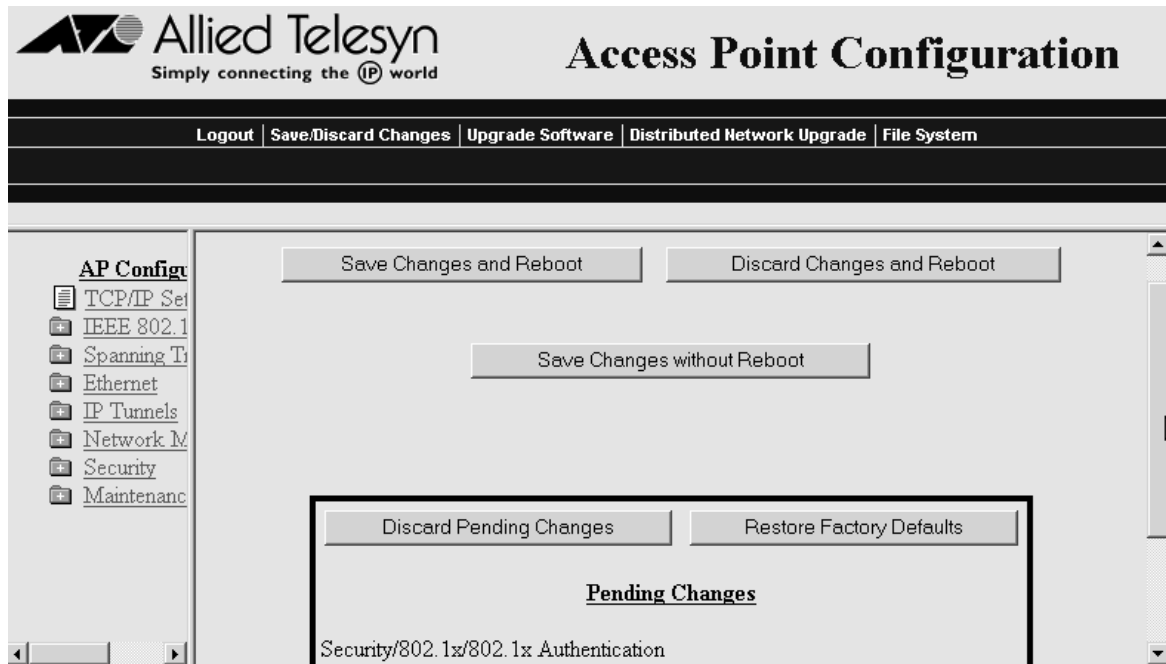


**Figure 64** About this Access Point Screen

## Restoring the Default Settings

You may need to restore the access point to the factory default configuration. This can be done using the Web browser interface. For a list of the default settings, see "Default Settings" in Appendix A. To restore the default configuration:

1. In the menu bar, click Save/Discard Changes. The Changes screen appears, as shown in Figure 64.



**Figure 65** Changes

2. Click Restore Factory Defaults. Under Pending Changes, you will see a list of what parameters need to be changed.
3. Click Save Changes and Reboot. When the access point is done rebooting, it will use the factory default settings as its active configuration. You may need to reset the IP address and other network parameters.

## Upgrading the Firmware

---

The procedures in this section explain how to upgrade the firmware on the AT-WL2411 to Version 1.72.

The current access point configuration information, such as IP address, should be retained when the new firmware is installed. However, keeping backup records of configuration settings is recommended.

You can install the firmware release using the following methods:

- ☐ Serial connection
- ☐ TFTP transfer via a Telnet session
- ☐ Web browser session (only available on Version 1.72 and later releases)

To upgrade the firmware, you must first download the firmware release onto your local computer. The latest version of the AT-WL2411 firmware is available from the Allied Telesyn Web site at [www.alliedtelesyn.com](http://www.alliedtelesyn.com).

### Using a Serial Connection

To upgrade the firmware using a serial connection, you must have an RS-232 null-modem cable connecting the wireless access point to your computer and a communications program such as HyperTerminal installed on your computer.

To upload the firmware, do the following:

1. Configure the following parameters on your communications software:

Baud rate	9600
Data bits	8
Parity	none
Stop bit	1
Flow control	none

2. Reboot the wireless access point and enter the wireless access point monitor by pressing any key within 5 seconds when prompted. The **ap>** prompt appears.
3. Type **srvc** at the prompt and press Enter.
4. Type the service password. The default password is EV98203S (case-sensitive). The **service>** prompt appears.
5. Type **fd** at the prompt and press Enter. The file directory appears.
6. Scroll up on the communications software window until you see a section similar to the following:

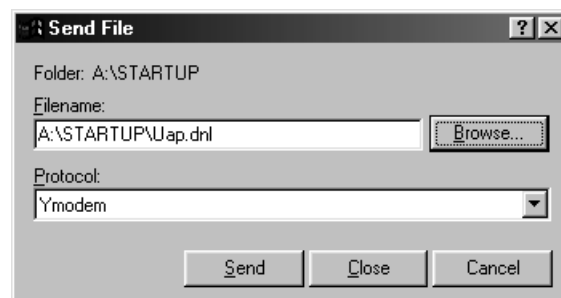
**Startup Segment: This startup = 1, Next startup = 1**

**Data Segment: This startup = 3, Next startup = 3**

7. These are the current startup and data segments. In this example, the active startup segment is 1 and the active data segment is 3.

You will first erase the inactive segments and then you will load the new firmware into the inactive segments and make those segments active. In this example, the inactive segments are 2 and 4.

8. Erase the inactive startup segment. Type **fe 2** at the **service>** prompt and press Enter. A **P** appears in the command line when the segment is erased.
9. Erase the inactive data segment. Type **fe 4** at the **service>** prompt and press Enter. A **P** appears in the command line when the segment is erased.
10. Transfer the startup files to the inactive startup segment.
  - a. At the **service>** prompt, type **fx s** (where **s** is the inactive startup segment) and press Enter. A series of **Cs** appears in the command line.
  - b. Click the Transfer menu tab in your communications program and then click Send File. The Send File dialog box appears, as shown below.



**Figure 66** Send File

- c. Click the Protocol down arrow and choose Ymodem.
  - d. Browse to the location where the UAP.DNL is saved. Double-click this file so that it appears in the Filename field.
  - e. Click Send to start the file transfer. A **P** appears in the command line when the transfer is complete.
11. Transfer the data files to the inactive data segment.

- a. At the **service>** prompt, type **fx s** (where **s** is the inactive data segment) and press Enter. A series of **Cs** appears in the command line.
  - b. Click the Transfer menu tab in your communications program and then click Send File. The Send File dialog box appears.
  - c. Browse to the location where the data files are saved. Double-click any data file. This file name appears in the Filename field.
  - d. To transfer all the data files at once, replace the specific file name with an asterisk (\*). For example, if the file name is c:\2411uap\data\applets.dnl, change it to c:\2411uap\data\\*.dnl.
  - e. Click Send to start the file transfer. A **P** appears in the command line when the transfer is complete.
12. Activate the inactive startup segment by typing **fb s** (where **s** is the inactive startup segment) at the **service>** prompt and pressing Enter. A **P** appears in the command line when the operation is complete.
  13. Activate the inactive data segment by typing **fb s** (where **s** is the inactive data segment) at the **service>** prompt and pressing Enter. A **P** appears in the command line when the operation is complete.
  14. Repeat steps 10 through 13 for the second startup file, uapboot.dnl.
  15. Type **x** at the **service>** prompt and press Enter to return to the **ap>** prompt.
  16. To reboot the wireless access point, type **b** and press Enter.
  17. Reconfigure the wireless access point, if necessary, and save the configuration. To activate the configuration, reboot the wireless access point.

## Using TFTP via Telnet

To upgrade the firmware using a TFTP transfer, you must have a TFTP server installed on your network. When you execute the UPGRADE.DNL script file that is included with the firmware release, a TFTP transfer copies all the startup and data files to the wireless access point.

To upgrade the firmware using a TFTP transfer, do the following:

1. Start your TFTP server.
2. Establish a Telnet session with the access point.
3. Choose the Maintenance command and then choose Command Console.
4. Use the **sdvars set serveripaddress** command to specify the IP address of the TFTP server. For example, if the server IP address is 151.60.110.241, type:

**sdvars set serveripaddress 151.60.110.241**

5. Use the `sdvars set scriptfilename` command to identify the script file. Type:

**`sdvars set scriptfilename c:\2411uap\upgrade.dnl`**

6. Use the `sdvars set starttime` command to set the start time for the upgrade in dd:hh:mm:ss format. Start time is a countdown time; when the timer expires, the download begins. You can enter days, hours, minutes, and seconds in the Start Time field. For example, to start the upgrade in two hours and ten minutes, type:

**`sdvars set starttime 00:02:10:00`**

When the starttime computer reaches zero, the upgrade begins. The wireless access point reboots after the upgrade is complete.

## Using a Web Browser

After you have downloaded the firmware release onto your computer, use the Web browser interface to upload the file from your PC to the wireless access point using the following procedures. **(Note: This option is only available when upgrading from Version 1.72 and later releases.)**

To upload the firmware, do the following:

1. Log into the wireless access point using the Web browser interface.
2. Click Upgrade Software. The Upgrade Software page appears, as shown in Figure 67 below.

**Figure 67** Upgrade Software



3. Enter the name of the upgrade file or click the Browse button to find the file on your computer.
4. Click the Upgrade button to start the upgrade. The upgrade may take up to three minutes to complete.
5. When the upgrade is complete, reboot the wireless access point to activate the new firmware.

For information on troubleshooting a Web browser firmware upgrade, refer to

## Chapter 9

# Troubleshooting

---

This chapter explains how to troubleshoot the access point.

### LEDs

---

When the access point is powered on, the LEDs flash as the access point boots and performs internal diagnostics. The table below describes the LED activity during the boot process.

Power	Radio	Wired LAN	Root/Error	Description
On	Off	Off	On	Flash checksum being calculated.
On	On	Off	On	Flash checksum failure.
On	Off	On	Off	RAM test in progress.
On	On	On	Off	RAM test failure.
On	Off	Off	Off	Monitor loading in progress.
On	Off	Off	On	Ethernet test in progress.
On	On	Off	On	Ethernet test failure

After the access point successfully boots, the LEDs display the following pattern:

<b>Power</b>	<b>Wireless #1</b>	<b>Wired LAN</b>	<b>Root/Error</b>
On	Flashes	Flashes	Flashes if the access point is configured as the root.

## Radio

---

**LEDs** If the radio is faulty or the configuration matrix string is incorrect, the LEDs on the access point display the following pattern after the access point boots:

Power	Radio	Wired LAN	Root/Error
On	Off	On	On

**Communications Program or Telnet** If you are connected to the access point through a serial connection, an error message also appears on your terminal or PC. The error messages are described in the following table.

**Table 3** Serial/Telnet Error Messages

Error Message	Explanation
Couldn't read country code from radio	The radio may be faulty. Contact your Allied Telesyn representative.
Radio A has unknown country code	The radio may have been configured incorrectly at the factory. Contact your Allied Telesyn representative.
Invalid country code in string for radio	The country code in the configuration matrix string does not match the country code in the radio in the access point. Contact your Allied Telesyn representative.
Radio string doesn't match radio installed	When this error message appears, additional information also appears on the screen. The radio may be faulty. Contact your Allied Telesyn representative.

**Radio MAC Ping** Radio MAC Ping runs at the MAC sublayer of the Data Link layer, thus allowing you to ping any 802.11b device that is connected to the access point. Radio MAC Ping can help you determine the connectivity and signal strength of an 802.11b radio.

To use radio MAC ping:

1. From the menu, click Maintenance and then click AP Connections. The AP Connections screen appears. All devices that support a radio MAC ping will have their MAC address listed with a hyperlink.

2. Click a MAC address hyperlink. The access point pings the device and then the Ping Utility screen appears showing the results.
3. Click Return to connections to return to the AP Connections screen.

**ICMP Echo**

ICMP (Internet Control Message Protocol) echo lets you ping devices using their IP address. ICMP echo can only be used if the access point has determined the IP address of the end device or another access point. If the access point is acting as an ARP server, it will determine the IP addresses of the end devices that are attached to it and allow you to use ICMP echo on the wireless network. The access point always knows the IP address of all access points in the spanning tree.

To use ICMP echo:

1. From the menu, click Maintenance and then click AP Connections. The AP Connections screen appears.
2. Click an IP address link. The access point pings the device and then the Ping Utility screen appears showing the results.
3. Click Return to connections to return to the AP Connections screen.

## Problems During Web Browser Firmware Upgrade

---

Each access point on a wired LAN requires approximately three minutes to upgrade (it takes slightly longer for wireless access points). The Web browser screen updates every 30 seconds as the upgrade progresses and shows the final status when all upgrades are complete. If you checked the Reboot selected Access Points after successful upgrade check box, the Web browser disconnects. Click the Refresh button to log in again. Errors may occur during the upgrade process or during the final reboot. If an error occurs, an explanation appears on the Web browser screen. If an error occurs during the upgrade, none of the access points reboot. You should:

1. Recheck the access points where the error occurred.
2. Click Start Upgrade to attempt the upgrade again. If the upgrade is successful and you checked the Reboot selected Access Points after successful upgrade check box, the access points will reboot.

If an error occurs during the final reboot, you should:

1. Wait five minutes for the access points that did not reboot to refresh.
2. Refresh your Web browser screen and check the access points that are not running the new version.
3. Press Start Upgrade to attempt the upgrade again. If the upgrade is successful and you checked the Reboot selected Access Points after successful upgrade check box, the access points will reboot according to your Reboot selection.

---

### Note

Only access points with Version 1.72 or higher firmware can upgrade using a Web browser.

---

## Commonly Asked Technical Support Questions

---

Refer to the following table for solutions and answers to common problems and questions concerning the AT-WL2411 unit.

<b>Problem/Question</b>	<b>Possible Solution/Answer</b>
Is the access point fully booted?	When the access point is fully booted, the Power LED remains steady green and the Wired LAN LED flashes.
The Power LED is not on.	<p>The access point may have a hardware problem.</p> <ol style="list-style-type: none"> <li>1. Make sure the power cable is firmly plugged into the access point and the power source.</li> <li>2. Unplug the access point, and then plug it back into the power source. Verify that the Power LED remains on.</li> <li>3. Call Allied Telesyn Technical Support.</li> </ol>
You cannot configure the access point locally using the serial port.	<ol style="list-style-type: none"> <li>1. Verify that you are using a null-modem cable to connect the access point to your terminal or PC.</li> <li>2. Verify that your terminal or PC is set to 9600, N, 8, 1, no flow control.</li> <li>3. Your system may be in autobaud mode. Reboot and press a key once per second until the signon screen appears.</li> </ol>
You cannot ping or Telnet to a new access point.	You must set an IP address and subnet mask using the serial port before you can remotely connect to the access point.
The Ping Utility screen does not appear when you click a MAC address or an IP address in the AP Connections screen.	The Web browser you are using does not have Java support. Use Internet Explorer v3.0 or later or Netscape Communicator v4.0 or later.
You cannot connect to the access point using a Web browser.	If you access the Internet through a proxy server, be sure you have added the IP address of the access point to the Exceptions list.
You cannot connect to the access point using an SNMP management station.	Verify that you did not disable the SNMP Access field in the Security screen.

**Problem/Question**

The end device cannot connect to the network.

The end device cannot synch to the access point.

The end devices are unable to roam to another AT-WL2411.

You need to verify the static WEP keys.

The filters are not filtering properly.

You need to verify the WEP keys.

You need to confirm which master a WAP is connected to.

**Possible Solution/Answer**

- ☐ Choose AP Connections from the Maintenance menu and verify that the MAC address of your end device appears on your PC screen. If it does not appear, your device is not communicating with the access point. Check your radio configuration settings.
- ☐ Verify that the access point is not filtering out the type of traffic you are trying to pass through it.

If you are using 802.11b HR radios:

- ☐ Verify that the end device and the access point have the same frequency and network name.

Roaming through switches requires backward learning, which is part of the IEEE 802.1D standard. If switches in your network do not support backward learning, you can create a data link tunnel to force all radio traffic through a fixed point so that roaming is transparent to the bridges or switches.

To create a data link tunnel:

1. Set Ethernet Bridging to Enable on the root access point.
2. Set Ethernet Bridging to Disabled on all access points that are separated from the root by a bridge or switch that does not support backward learning.

You cannot verify the WEP keys. The keys are encrypted after you enter them and are never displayed again. You may need to reconfigure your access points and end devices to reset the WEP keys.

Check all of your filter settings. Conflicts may exist between the various filters.

You cannot verify the WEP keys. The keys are encrypted after you enter them and are never displayed again. You may need to reconfigure your access points and end devices to reset the WEP keys.

To verify that a WAP is communicating with a particular access point, view the AP Connections screen for the access point. Click Maintenance, and then click AP Connections.



**Problem/Question**

You cannot establish an IP tunnel to a access point on a remote subnet.

**Possible Solution/Answer**

1. Click TCP/IP Settings and verify that the IP Router (Gateway) address is correct.
2. Click Spanning Tree Settings and verify that the access points on both ends of the tunnel have the same LAN ID.
3. Click IP Addresses from the IP Tunnels menu to verify that the IP address of the remote access point appears in the IP Addresses list.

The throughput seems slow.

- ☐ Verify that your antennas are well placed and that they are not blocked by metal or other obstacles.
- ☐ You may want to add a second access point and implement roaming if you move the antenna closer to the device and throughput increases.

You may be able to set filters to eliminate Ethernet traffic on the wireless side of the network.

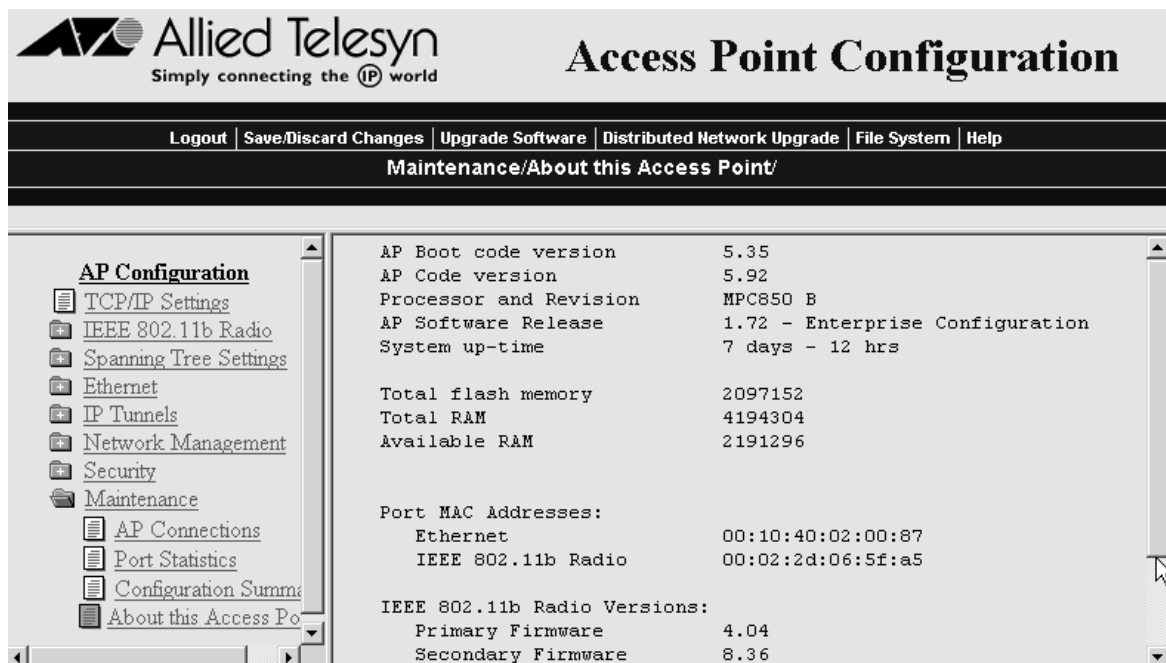
## Getting Help with Your Installation

The AT-WL2411 access point is designed to be easy to install and configure; however, you may need to call Allied Telesyn Technical Support if you have problems. Before calling, be sure you can answer the following questions:

- ☐ What kind of network are you using?
- ☐ What were you doing when the error occurred?
- ☐ What error message did you see?
- ☐ Can you reproduce the problem?
- ☐ What version of the firmware are you using?

To confirm the firmware version on your access point, do the following:

1. Establish a Web browser session.
2. Click Maintenance and then click About this Access Point. The About this Access Point screen appears, as shown in Figure 68.



**Figure 68** About this Access Point Screen

You should have the information on this screen available when you call Allied Telesyn Technical Support.

## Chapter 10

# Advanced Configuration Commands

---

This chapter describes the access point monitor, console command mode, and how to use script files to update the system files.

## Using the Access Point Monitor

---

The access point monitor is the system software that controls the access point. You can use access point monitor commands to manipulate the access point file segments.

### Understanding Access Point Segments

The access point has the following five segments in its file system:

- ☐ The current active boot or startup segment (can be segment 1 or 2)
- ☐ The current inactive boot or startup segment (can be segment 1 or 2)
- ☐ The current active data segment (can be segment 3 or 4)
- ☐ The current inactive data segment (can be segment 3 or 4)
- ☐ The RAM memory segment

You can enter commands to manipulate the boot and data segments. For instance, you typically download a new firmware version into an inactive segment and then make that segment active the next time the access point boots. For more information on upgrading the access point firmware, see **Upgrading the Firmware** on page 141.

## Entering the Access Point Monitor

You can enter the access point monitor only through a connection on the serial port and only during the boot process.

To enter the access point monitor, do the following:

- ☐ Press any key on the keyboard when you see this message displayed during the boot process:

```
<Press any key within 5 seconds to enter the  
access point monitor>
```

---

### Note

Certain functions available through the access point monitor can erase your configuration information. Allied Telesyn strongly recommends that you only use the access point monitor when absolutely necessary. For example, you might use the access point monitor to upgrade your firmware or when instructed to do so by qualified Allied Telesyn personnel.

---

# Using Access Point Monitor Commands

When you are in the access point monitor, the access point prompt (uap>) appears. You can display a list of access point monitor commands anytime you see the access point prompt.

To display access point monitor commands, do the following:

- ❑ Press a letter or number key on the keyboard, and then press Enter. A list of access point monitor commands appears.

**Note**

If you type the letter B (upper or lower case) and press Enter, the access point will reboot. Type any letter or number OTHER than B to display access point commands.

The following example shows the list of available access point commands. The commands are not case sensitive; you can type the commands using either upper or lower case.

```
UAP Monitor V4.03 July 17,2000
<Press any key within 5 seconds to enter the UAP monitor>
uap>d
-----
----"uap>" commands...
-----
-----
B          -Reboot                               |          -Device IDs
menu
FX s      -Ymodem File Download                 | MR        -Display
Mfg Record
FD        -File System Directory                 | TEST      -Test Menu
FR        -Run Flash Startup File                | SRVC      -Service Menu
          -Manufacturing Menu                   | SR z      -Serial Baud Rate
-----
-----
uap>
```

**B Purpose**

Deletes the most recent data record and remains in Accumulate mode. If no data exists, a null string is entered.

**Syntax**

B

**FX Purpose**

Performs a Ymodem batch protocol download of a file into the flash segment that is specified by *s*.

**Syntax**

FX *s*

where *s* is segment 1, 2, 3, or 4.

**FD Purpose**

Displays the flash file system directory, including information about the boot file.

**Syntax**

FD

**FR Purpose**

Finds the first executable file in the access point boot segment and tries to run it; therefore, the first executable file in the access point boot segment must be the boot file.

**Syntax**

FR

**MR Purpose**

Displays the manufacturing record for the access point. Use the MR command to display the MAC address, configuration string, and serial number for your access point.

**Syntax**

MR

**SR Purpose**

The SR command sets the baud rate of the access point.

**Syntax**

SR *z*

where *z* is the baud rate.

You must enter the baud rate as a whole number with no commas. For example, to enter a baud rate of 19,200, you must enter 19200.

### **Setting Autobaud Using the SR Command**

You can use autobaud to let the access point set its baud rate to match the baud rate of your terminal, up to a baud rate of 115,200.

To set Autobaud using SR, do the following:

1. Set the baud rate to 0 using SR.
2. Press Enter twice. The autobaud feature automatically detects the baud rate of your terminal and sets the baud rate of the access point to match.

## Using Service Mode Commands

Use service mode to perform certain file functions. Because service mode commands can cause undesirable results if not properly executed, you should contact Allied Telesyn Technical Support for assistance if you are unsure about the proper procedure to use.

**SRVC** Use the SRVC command to enter service mode. In service mode, you can perform file functions such as deleting a file and performing a Ymodem download through the serial port.

To enter service mode, do the following:

1. Type SRVC and press Enter.
2. Enter a password. The default password is EV98203S (case sensitive).

When you are in service mode, the service prompt (service>) appears. Service mode has a set of defined commands that you can use.

To display service mode commands, do the following:

- ☐ Type any letter or number (other than B) and press Enter. The service commands appear on the screen.

```

UAP Monitor V4.03 July 17,2000
Press any key within 5 seconds to enter the UAP monitor>
uap>srvc
Enter password : *****
service>d
-----
--"service"> commands...
-----
--FD          - File System Directory | SU b      - Set Upgrade Byte
FDEL f (s)- File Delete                | RU        - Reset Upgrade
Bytes
FE <s|all>- Erase Segment(s)           | DU        - Display Upgrade
Bytes
FI           - File System Reset       | PN        - Normal power up
FFR f (s) - Run File                   | PQ        - Quiet power up
FX s       - Ymodem File Download     | B         - Reboot
FB bs (ds)- Set Boot/Data Segments | X         - Exit
-----
--

```

Most of the commands that you use in service mode are also used in the access point monitor or console command mode and are described in those sections in this chapter. Some additional service commands you may need are listed next.



## **FFR Purpose**

Runs a program that is specified by *f*, from a location specified by *s*.

### **Syntax**

FFR *f* (*s*)

where:

*f* is the program name.

*s* is the optional segment location of the program.

Example: To run program access pointBOOT.PRG from segment 1, enter:

```
FFR access pointBOOT.PRG 1
```

## **PN Purpose**

Returns the access point to normal mode from quiet mode.

### **Syntax**

PN

To return the access point to normal mode

1. Reboot the access point.
2. The LEDs flash on and off during the reboot. When the LEDs flash off and only the Power LED remains lit, type !!! (three exclamation points). The access point prompt (access point>) appears.
3. Type SRVC and press Enter.
4. Type the service password (the default is EV98203S) and press Enter. The service prompt (service>) appears.
5. Type PN and press Enter.
6. Type B to reboot the access point in normal mode.

## **PQ Purpose**

Puts the access point in quiet mode. When the access point is in quiet mode, you cannot access the access point monitor. You may want to use quiet mode for security reasons.

### **Syntax**

PQ

## Using Test Mode Commands

---

Within the access point monitor, test mode allows you to perform certain test functions. Because the commands can cause undesirable results if not properly executed, you should contact Allied Telesyn Technical Support for assistance if you are unsure about the proper procedure to use.

### **TEST      Purpose**

Allows you to enter test mode where you can perform a variety of test functions.

### **Syntax**

TEST

To enter test mode, do the following:

1. Type TEST and press Enter.
2. Enter a password. The default password is EV98203T (case sensitive).

When you are in test mode, the test prompt (test>) appears. Test mode has a set of defined commands that you can use.

To display test mode commands, do the following:

- ❑ Type any letter or number other than B and press Enter. The test commands appear on the screen.

```
UAP Monitor V4.03 July 17, 2000
<Press any key within 5 seconds to enter the UAP monitor>
uap>test
Enter password : *****
test>d
-----
-----"test"> commands...
-----
-----
LT          - LED Test          | MWW s d .. d - Memory word
Write
MACE        - MACE Test Menu    | MRB s l      - Memory byte
Read
MF s l      - Memory Fill       | MWB s d .. d - Memory byte
Write
MV s l      - Memory Verify     | SD           - Get DRAM Size
(K)
MR s l      - Memory dword Read | SF           - Get Flash Size
(K)
MW s d .. d - Memory dword Write| X            - Exit
MRW s l     - Memory word Read
-----
-----
test>
```

## Using Console Command Mode

---

Another way you can access the access point file system is through Console Command mode. Use Console Command mode to upgrade access points using TFTP and Script files.

To enter Console Command mode, do the following:

- ☐ Choose Command Console from the Maintenance menu.

When you first enter Console Command mode, a list of valid console commands appears. You can display the console commands any time you are in Console Command mode.

To display console commands, do the following:

- ☐ Type F and press Enter. The following screen appears.

Command	Description
=====	=====
Fb	fb <boot segment> <data segment>
Fd	fd (<segment>   all) - directory list
Fdel	fdel <filename> - delete file
Fe	fe (<segment>   all) - erase
segment(s)	
Tftp	File transfer
Script	Execute script files
SDVars	Software Download variables
Exit	Return to main menu
?	Display this help

To exit Console Command mode, do the following:

- ☐ Type exit and press Enter.

Several file menu commands require that you enter file names. To indicate the segment where the file is located, precede the file name with either a segment number or name followed by a colon. For example:

```
1:access point.prg
```

refers to the file named access point.PRg that is located in segment 1. If you do not specify a segment name or number, the access point searches the segments in the following order until it finds a file that matches the file name:

RAM, 1, 2, 3, 4

## Using Console Commands

---

This section describes the console commands.

### **fb Purpose**

Use the fb command to make an inactive segment the active segment.

### **Syntax**

```
fb boot segment data segment
```

where:

boot segment            is the name or number of the boot segment to be activated.

data segment            is the name or number of the data segment to be activated.

### **Example**

To make segment 2 the active boot segment and segment 4 the active data segment, enter:

```
fb 2 4
```

You can use an asterisk instead of a segment name if you want to leave that segment unchanged. For example, to leave the active boot segment unchanged and make segment 4 the active data segment, you could enter:

```
fb * 4
```

After loading software into the access point a common task is to activate the new software. To activate the new software, enter:

```
Fb ib: id:
```

This command activates the inactive boot and data segments. You do not need to know which of the boot and data segment numbers the flash is loaded into.

**fd Purpose**

Use the fd command to display the flash file system directory, which includes information about the boot file.

**Syntax**

```
fd
```

Use the fd command to ensure that the correct version of the file is in the active boot segment.

Typing fd ab: shows only the files loaded in the active boot segment.

**Note**

If the active segment contains no files when you reboot the access point, the unit enters the access point monitor and you lose the ability to Telnet to it during this session. If this occurs, you must access the access point through its serial port to correct the problem.

**fdel Purpose**

Use the fdel command to delete a particular file name from a segment.

**Syntax**

```
fdel filename
```

where filename is the name of the file to be deleted.

**Example**

To delete the file access point.PRG from the inactive boot segment, enter:

```
fdel ib:access point.prg
```

**Note**

When you use the fdel command, the file is marked as invalid and remains in the file system. To reclaim the file space, you must erase the entire segment. Use the fe command to erase a segment.

## **fe Purpose**

Erases the files in a particular segment. To recover the files after they have been erased, you must reload them from another source.

### **Syntax**

```
fe segment
```

where *segment* is the name or number of the segment to be erased.

### **Example**

To erase the contents of segment 1, enter:

```
fe 1
```

You can enter ALL instead of a segment name or number if you want to erase segments 1 through 4.

Fe ib: erases the contents of the inactive boot segment.

---

#### **Note**

You must execute the fe command before you execute a TFTP transfer.

---

## **script Purpose**

Executes a specified file as a list of console commands. You can create a script file to automate a software download.

### **Syntax**

```
script filename
```

where *filename* is the name of the script file to be executed.

## Using Sdvars Commands

---

Use sdvars commands in Console Command mode to manipulate certain software download variables. Sdvars commands support both GET and SET arguments. You can enter sdvars commands to GET a software download object, and then issue the sdvars command using the SET argument to assign the object a specified value.

The sdvars commands are described in this section using the SET argument. To execute an sdvars command using the GET argument, omit the variable from the end of the command.

### **sdvars set serveripaddress**

#### **Purpose**

Sets the internal variable called serveripaddress to a specified address.

#### **Format**

```
sdvars set serveripaddress ip address
```

where *ip address* is the address of the server.

#### **Example**

To set the IP address of the server to 192.168.49.29, enter:

```
sdvars set serveripaddress 192.168.49.29
```

### **sdvars set scriptfilename**

#### **Purpose**

Sets the internal variable scriptfilename to a specified string. The specified string should be the filename of the script to be retrieved from the TFTP server.

#### **Syntax**

```
sdvars set scriptfilename foreign filename
```

where *foreign filename* is a script filename on the TFTP server.

#### **Example**

To set the scriptfilename to SCRIPT.DAT, enter:

```
sdvars set scriptfilename script.dat
```



## **sdvars set starttime**

### **Purpose**

Sets the internal variable starttime. Starttime is a countdown time such that when zero is reached, the software download process begins. You set this variable to reflect how long into the future the access point is to begin downloading and executing the script file from the TFTP server. When the timer reaches 0, the access point uses the values in serveripaddress and scriptfilename to get the script file that is to be executed. If either serveripaddress or scriptfilename contains no value, an error is noted in the status variable and the software download process is terminated.

### **Syntax**

```
sdvars set starttime dd:hh:mm:ss
```

where *dd:hh:mm:ss* is how far in the future the download is to begin.

### **Example**

To begin the script file download in 5 minutes, enter:

```
sdvars set starttime 00:00:05:00
```

---

#### **Note**

If you need to stop the download, you can do so by setting starttime to 0 if it has not already been reached by the countdown. Resetting starttime to 0 stops the timer and the download process.

---

## **sdvars set checkpoint**

### **Purpose**

Sets the internal variable called checkpoint to a specified value. The checkpoint variable is useful for monitoring the progress of a script file as it is executed. You can set the checkpoint variable to a different value after each script command and then query the checkpoint value using SNMP to determine the progress of the download.

### **Syntax**

```
sdvars set checkpoint value
```

where *value* is a whole number.

## Example

Consider the following script file commands:

```
sdvars set checkpoint 1
fe ab
sdvars set checkpoint 2
TFTP get * access point.prg ab
sdvars set checkpoint 3
reboot
```

When the software download is started, you can use SNMP to query its progress by reading the checkpoint variable. If the variable has a value of 2, you know that the access point is trying to execute the TFTP get statement. If the value is 3, you know the script has completed and the reboot was executed. The value of the checkpoint variable may also be helpful in determining where an error occurred if the script fails.

### **sdvars set terminate**

#### **Purpose**

Sets the internal variable terminate to a specified value. Use terminate to stop a countdown process in the access point. If either starttime or nextpoweruptime is counting down, setting this variable stops the timer and halts the countdown process.

#### **Syntax**

```
sdvars set terminate
```

---

#### **Note**

You should use caution when using this command. If the script file is being downloaded or executed, setting this variable interrupts the processing and can leave the access point in an undetermined state that may require user intervention.

---

### **sdvars set setactivepointer s**

#### **Purpose**

Sets the setactivepointers command to change inactive segments to active segments the next time the access point is rebooted. This command is usually used with the nextpoweruptime command.

#### **Syntax**

```
sdvars set setactivepointers none/boot/data/both
```

where:

none	does not change the active segments. The default is none. Also, when the reboot is completed, the access point resets this value to none.
boot	changes the inactive boot segment to the active boot segment.
data	changes the inactive data segment to the active data segment.
both	changes both the boot and data inactive segments to the active segments.

### Example

To change the inactive boot and data segments to active at the next reboot, enter:

```
sdvars set setactivepointers both
```

### sdvars set nextpoweruptime

#### Purpose

Sets the nextpoweruptime command to set the internal variable nextpoweruptime to a countdown time so that when 0 is reached, the access point will reboot. When the nextpoweruptime counter reaches 0, the access point checks the value of the setactivepointers variable, takes the appropriate action, and then reboots.

#### Syntax

```
sdvars set nextpoweruptime dd:hh:mm:ss
```

where dd:hh:mm:ss is how far in the future the reboot is to begin.

### Example

To reboot the access point 2 hours from now, enter:

```
sdvars set nextpoweruptime 00:02:00:00
```

---

#### Note

If you need to terminate the reboot, you can do so by setting nextpoweruptime to 0 if it has not already been reached by the countdown. By resetting nextpoweruptime to 0, the timer is stopped so the unit does not reboot.

---

## Using TFTP Commands

---

TFTP commands are file transfer commands that you execute when you are in Console Command mode. A access point can act as either a client or server in the TFTP environment. As a server, the access point can service read and write requests from a access point client. As a client, the access point can read files from and write files to any TFTP server on the network. Both the client and server must operate in octet, or 8-bit, mode.

When executing a script file, the access point retries TFTP client commands get and put until the command is successfully completed. If the first attempt fails, the access point retries after a one-minute delay. With each successive failure, the retry time doubles until it reaches eight minutes. Once this limit is reached, it remains at eight minutes until the command is completed.

In general, TFTP client sessions should fail only if the server is not responding either because it is busy serving other clients or because it has not been started. In either case, the access point backoff algorithm should prevent excessive network traffic when many access points are trying to contact a TFTP server.

### **tftp get**      **Purpose**

Supports standard get and put commands. You can use the TFTP get command to start a client session that gets a file from the TFTP server.

### **Syntax**

`tftp get IP address foreign filename local filename`

where:

IP address	is the IP address of the server. You can use an asterisk (*) here if you want to use the value in serveripaddress.
foreign filename	is the name of the file on the server. The filename can contain directory path information and must be in the format required by the server operating system. The file must already have the appropriate file header before the transfer to the access point.

local filename is the name you wish to call the file on the access point. The name must include a segment number or name followed by a colon. An actual filename is optional. If only the segment name is supplied, the filename is set equal to the filename that is embedded in the file header on the server.

### Example

The following command gets file access point.DNL from a directory on a PC server with IP address 1.2.3.4 and stores it in the inactive boot segment on the access point.

```
tftp get 1.2.3.4 c:\startup\access point.dnl ib:
```

---

#### Note

You must use the fe command to erase the segment before you execute a TFTP get command. If you do not erase the segment, you may get a "can't write file" error.

---

The following error messages may be generated by the access point when the access point issues a TFTP get command. Other error messages may be returned from the server and displayed by the access point. See your server documentation for additional information.

Error Message	Explanation
Can't write file	The file may be too big.
	The file may not have a access point file header (filehdr.exe).
	The file name may be incorrectly formed.
	The file may already exist in the segment and cannot be overwritten. You must erase the file first.
Invalid opcode during read	This error should not occur under normal operating conditions. This error indicates a TFTP protocol error that will not occur when you use TFTP servers that conform to the protocol.

**tftp put    Purpose**

Copies a file from a client to the server or to another access point.

**Syntax**

`tftp put IP address foreign filename local filename`

where:

IP address	is the IP address of the server. You can use an asterisk (*) here if you want to use the value in the serveripaddress.
foreign filename	is the name of the file as it will appear on the server. The file name can contain directory path information and must be in the format required by the server operating system.
local filename	is the name of the file to be sent from the access point.

**Example**

The following command takes file access point.PRG that is saved in the active boot drive on the access point client and stores it in the inactive boot segment on the access point server that has IP address 1.2.3.4.

```
tftp put 1.2.3.4 ib:access point.prg ab:access
point.prg
```

The following error messages may be generated by the access point when the access point issues a TFTP put command. Other error messages may be returned from the server and displayed by the access point. See your server documentation.

Error Message	Explanation
Can't read file	The requested file may not exist.
Invalid opcode during put	This error should not occur under normal operating conditions. This error indicates a TFTP protocol error that will not occur when you use TFTP servers that conform to the protocol.

## **tftp server log**      **Purpose**

Your access point can function as a TFTP server. You can use the TFTP server log command to save a history of TFTP client requests.

### **Syntax**

```
tftp server log
```

The TFTP server log contains useful TFTP server status information. The log begins when you set up the server. You must reboot the access point to clear the log.

## **tftp server start**      **Purpose**

A access point can obtain files from a TFTP server. You can enable one access point to act as a TFTP server and download files to additional access points. Use the TFTP server start command to enable your access point to act as a server.

### **Syntax**

```
tftp server start
```

After you issue this command, the access point responds to TFTP client requests that are directed to its IP address. When acting as a server, the access point supports up to four concurrent TFTP sessions.

## **tftp server stop**      **Purpose**

When you are done transferring files, you can stop the access point from being a TFTP server by using the TFTP server stop command.

### **Syntax**

```
tftp server stop
```

After you issue this command, the access point no longer responds to TFTP client requests; however, current TFTP sessions with the server are allowed to complete.

The following table lists error messages that can be issued from the TFTP server. These messages are sent to the client and are meant to be read from the client perspective.

Error Message	Explanation
TFTP server only supports octet mode	The client is attempting to transfer a file in ASCII mode. The access point TFTP server only supports octet mode, which includes binary and image.
Unable to open remote file	<p>The TFTP server cannot open the file that is named in the read or write request.</p> <p>If you are trying to read a file, the file may not exist.</p> <p>If you are trying to write a file, the file may be too big, the file may not have a access point file header, or the file name may be incorrectly formed.</p>
Can't read remote file	The server returns this message if the access point file system returns an error while the server is attempting to read the file. This message is unlikely to occur.
Can't write remote file	The server returns this message if the access point file system returns an error while the server is attempting to write the file. This message is unlikely to occur.
TFTP opcode not read or write request	This error should not occur under normal operating conditions. This error indicates that the TFTP client does not conform to the protocol.
Invalid opcode during read	This error should not occur under normal operating conditions. This error indicates that the TFTP client does not conform to the protocol.
Invalid opcode during write	This error should not occur under normal operating conditions. This error indicates that the TFTP client does not conform to the protocol.





## Appendix A

# Default Configuration Settings

---

### TCP/IP Menu Default Settings

---

Parameter Name	Range	Default
IP Address	4 nodes, 0 to 255	0.0.0.0
IP Subnet Mask	4 nodes, 0 to 255	255.255.255.0
IP Router (Gateway)	4 nodes, 0 to 255	0.0.0.0
IP Frame Type	DIX/SNAP	DIX
Auto ARP Minutes	0 to 120	5
ARP Server Mode	Disabled, No Flooding, or Normal Flooding	Disabled
DHCP Mode	Always use DHCP, Use DHCP if IP Address is Zero, Disable DHCP, This is a DHCP Server	Use DHCP if IP Address is Zero
DHCP Server Name	0 to 31 characters	(blank)

## IEEE 802.11b Radio Menu Default Settings

---

Parameter Name	Range	Default
Port Control	Enabled/Disabled	Enabled
SSID (Network Name)	0 to 32 characters	ATILAN
Frequency	Channel 1 to 14, 2400 to 2500 MHz	Channel 3, 2422 MHz
Data/Voice Settings	Data Only, Data and Voice, or Voice Only	Data Only

### Wireless Bridging

Node Type	Station/Master	Master
Wireless Hops	Enabled/Disabled	Disabled

### Advanced Configuration

Data Rate	11, 5.5, 2, or 1 Mbps	11 Mbps (High)
Data Rate Fallback	Enabled/Disabled	Enabled
Basic Rate	11, 5.5, 2, or 1 Mbps	2 Mbps (Standard)
Medium Reservation	Enabled/Disabled	Disabled
Distance Between APs	Large, Medium, or Small	Large
Microwave Oven Robustness	Enabled/Disabled	Disabled
Network Name Security	802.11 compliant/ Network Name "ANY" not allowed	802.11 compliant
DTIM Period	1 to 65535	1
Load Balancing	Enabled/Disabled	Disabled
Medium Density Distribution	Enabled/Disabled	Disabled

## Spanning Tree Settings Menu Default Settings

---

Parameter Name	Range	Default
AP Name	0 to 16 characters	(access point serial number)
LAN ID (Domain)	0 to 254	0
Root Priority	0 to 7	1
IAPP Frame Type	DIX/SNAP	DIX
Ethernet Bridging	Enabled/ Disabled	Enabled
Secondary LAN Bridge Priority	0 to 7	0
Secondary LAN Flooding	Enabled/Disabled	Disabled

### Global Flooding

Multicast Flood Mode	Universal, Hierarchical, or Disabled	Hierarchical
Multicast Outbound to Terminals	Enabled/ Disabled	Enabled
Multicast Outbound to Secondary LANs	Enabled/Set Locally	Set Locally
Unicast Flood Mode	Universal, Hierarchical, or Disabled	Disabled

## Global RF Parameters

Parameter Name	Range	Default
RFC1042/DIX Conversion	Enabled/Disabled	Enabled

### RFC1042 Types to Pass Through

1	Two sets of hexadecimal pairs 00 through FF	80 F3
2	Two sets of hexadecimal pairs 00 through FF	81 37
3 through 20	Two sets of hexadecimal pairs 00 through FF	00 00

## Ethernet Menu Default Settings

---

Parameter Name	Range	Default
Hello Period	1, 2, or 3 seconds	2

### Address Table

1 through 20	Six sets of hexadecimal pairs 00 through FF	00:00:00:00:00:00
--------------	---	-------------------

### Frame Type Filters

Action	Pass/Drop	Pass
Scope	Unlisted/All	Unlisted
Predefined Subtype Filters		
Action	Pass/Drop	Pass
Customizable Subtype Filters		
Action	Pass/Drop	Pass
Subtype	DIX-IP-TCP-Port, DIX-IP-UDP-Port, DIX-IP-Protocol, DIX-IPX-Socket, DIX-EtherType, SNAP-IP-TCP-Port, SNAP-IP-UDP-Port, SNAP-IP-Protocol, SNAP-IPX-Socket, SNAP-EtherType, 802.3-IPX-Socket, 802.2-IPX-Socket, or 802.2-SAP	DIX-IP-TCP-Port

## Predefined Subtype Filers

Parameter Name	Range	Default
Action	Pass/Drop	Pass

## Customizable Subtype Filters

Action	Pass/Drop	Pass
Subtype	DIX-IP-TCP-Port, DIX-IP-UDP-Port, DIX-IP-Protocol, DIX-IPX-Socket, DIX-EtherType, SNAP-IP-TCP-Port, SNAP-IP-UDP-Port, SNAP-IP-Protocol, SNAP-IPX-Socket, SNAP-EtherType, 802.3-IPX-Socket, 802.2-IPX-Socket, or 802.2-SAP	DIX-IP-TCP-Port
Value	Two sets of hexadecimal pairs 00 through FF	00 00

## Advanced Filters

### Filter Values

Value ID	0 - 22	0
Value	0 - 8 hexadecimal pairs	(blank)

### Filter Expressions

ExprSeq	0 - 255	0
Offset	0 - 65535	0
Mask	0 - 8 hexadecimal pairs	(blank)
Op	EQ, NE, GT, or LE	EQ
Value ID	0 - 255	0
Action	And, Pass, or Drop	And

## IP Tunnels Menu Default Settings

---

Parameter Name	Range	Default
Port Control	Enabled/Disabled	Enabled
Mode	Listen/Originate If Root	Originate If Root
IGMP	Enabled/Disabled	Disabled
Hello Period	1, 2, or 3 Seconds	2

### Tunnel Filters

#### Frame Type Filters

Action	Pass/Drop	Drop
Scope	Unlisted/All	Unlisted

#### Predefined Subtype Filters

Action	Pass/Drop	Drop (except Pass for NNL)
--------	-----------	----------------------------

#### Customizable Subtype Filters

Action	Pass/Drop	Drop
Subtype	DIX-IP-TCP-Port, DIX-IP-UDP-Port, DIX-IP-Protocol, DIX-IPX-Socket, DIX-EtherType, SNAP-IP-TCP-Port, SNAP-IP-UDP-Port, SNAP-IP-Protocol, SNAP-IPX-Socket, SNAP-EtherType, 802.3-IPX-Socket, 802.2-IPX-Socket, or 802.2-SAP	DIX-IP-TCP-Port
Value	Two sets of hexadecimal pairs 00 through FF	00 00



## Network Management Menu Default Settings

---

### Community Strings

Parameter Name	Range	Default
SNMP Read Community	1 to 15 characters	public
SNMP Write Community	1 to 15 characters	CR52401
SNMP Secret Community	1 to 15 characters	Secret

## Security Menu Default Settings

---

Parameter Name	Range	Default
Telnet Access	Enabled/Disabled	Enabled
Browser Access	Enabled/Disabled	Enabled
SNMP Access	Enabled/Disabled	Enabled
ICMP Configuration	Enabled/Disabled	Enabled

### Passwords

RADIUS Authorization	Enabled/Disabled	Disabled
User Name	1 to 16 characters	ATILAN
Password	1 to 16 characters	ATILAN
Read Only Password	1 to 16 characters	(blank)
Service Password	Enabled/Disabled	Enabled

### 802.1x

802.1x Authentication	Enabled/Disabled	Disabled
-----------------------	------------------	----------

### IEEE 802.11b Radio WEP

WEP Encryption	Enabled/Disabled	Disabled
----------------	------------------	----------

### Internal RADIUS Server

Server	Enabled/Disabled	Disabled
--------	------------------	----------

## Appendix B

# Technical Specifications

---

### Physical Specifications

---

Dimensions (HxDxW)	9.32 cm x 14.66 cm x 3.53 cm (3.67 in. x 5.77 in. x 1.39 in.)
Weight	232 g (0.51 lbs)
Recommended Minimum Ventilation on All Sides	5.08 cm (2.0 in.)

### Environmental Specifications

---

Operating Temperature	-20° C to 65° C (-4° F to 149° F)
Storage Temperature	-40° C to 70° C (-40° F to 158° F)
Humidity	10% to 90% non-condensing

### Power Specifications

---

AC Input Voltage	2 A
Input Supply Voltage	5 V DC

### Safety and Electromagnetic Emissions Certifications

---

Safety	EN60950 (TUV), UL1950 (UL/cUL)
EMI	FCC Class B, EN55022 Class B
Immunity	EN55024

### Standards

---

IEEE 802.3 10Base-T Ethernet and CSMA/CD

## Other Specifications

---

Architecture	transparent bridge
Data Rate	10 Mbps (Ethernet)
Filtering Rate	14,880 frames per second
Filters (Protocol)	Appletalk, NetBEUI, IPX, IP, DECNET
Filters (Other)	IP ARP, Novell RIP, SAP, LSP
Serial Port Max Data Rate	115, 200 bps
Management Interfaces	SNMP, Web, Telnet, Serial Connection
SNMP Agent	Version 1 RFC1213,1493, Enterprise MIB
Software Upgrades	Web, TFTP via Telnet, Serial Connection

## IEEE 802.11b Radio Specifications

---

Frequency Band	2.4 to 2.5 GHz worldwide
Type	direct sequence, spread spectrum
Modulation	direct sequence, spread spectrum (CCK, DQPSK, DBPSK)
Power Output	32 mW (15 dBm)
Data Rate	11 Mbps (High), 5.5 Mbps (Medium), 2 Mbps (Standard), 1 Mbps (Low) with automatic fallback for increased range
Channels	11 (North America), 13 (Europe), 4 (France), 14 (Japan), 1 (Israel)
Range (11 Mbps)	160 m (525 ft) open environment, 50 m (165 ft) semi-open environment, 24 m (80 ft) closed environment
Receiver Sensitivity (11 Mbps)	-82 dBm
Security	IEEE 802.11 Wired Equivalent Privacy (WEP) standard, WEP 64, WEP 128

## Appendix C

# Translated Electrical Safety and Emission Information

---

**Important:** This appendix contains multiple-language translations for the safety statements in this guide.

**Wichtig:** Dieser Anhang enthält Übersetzungen der in diesem Handbuch enthaltenen Sicherheitshinweise in mehreren Sprachen.

**Vigtigt:** Dette tillæg indeholder oversættelser i flere sprog af sikkerhedsadvarslerne i denne håndbog.

**Belangrijk:** Deze appendix bevat vertalingen in meerdere talen van de veiligheidsopmerkingen in deze gids.

**Important:** Cette annexe contient la traduction en plusieurs langues des instructions de sécurité figurant dans ce guide.

**Tärkeää:** Tämä liite sisältää tässä oppaassa esiintyvät turvaohjeet usealla kielellä.

**Importante:** questa appendice contiene traduzioni in più lingue degli avvisi di sicurezza di questa guida.

**Viktig:** Dette tillegget inneholder oversettelser til flere språk av sikkerhetsinformasjonen i denne veiledningen.

**Importante:** Este anexo contém traduções em vários idiomas das advertências de segurança neste guia.

**Importante:** Este apéndice contiene traducciones en múltiples idiomas de los mensajes de seguridad incluidos en esta guía.

**Obs!** Denna bilaga innehåller flerspråkiga översättningar av säkerhetsmeddelandena i denna handledning.

**Standards:** This product meets the following safety standards.



U.S. Federal Communications Commission	
<b>Declaration Of Conformity</b>	
Manufacture Name:	Allied Telesyn, Inc.
Manufacture Address:	960 Stewart Drive, Suite B Sunnyvale, CA 94085 USA
Manufacture Telephone:	408-730-0950
Declares that the product:	Access Point
Model Numbers:	AT-WL2411
This product complies with FCC Part 15B, Class B Limits:	
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device must not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.	
<b>Radiated Energy</b>	
Note: This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with instructions, may cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on. The user is encouraged to try to correct the interference by one or more of the following measures:	
<ul style="list-style-type: none"> <li>- Reorient or relocate the receiving antenna.</li> <li>- Increase the separation between the equipment and the receiver.</li> <li>- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.</li> <li>- Consult the dealer or an experienced radio/TV technician for help.</li> </ul>	
Changes and modifications not expressly approved by the manufacturer or registrant of this equipment can void your authority to operate this equipment under Federal Communications Commission rules.	

Canadian Department of Communications
<p>This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.</p> <p>Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.</p>

**Standards:** This product meets the following safety standards.

 1	RFI Emission	EN55022 Class B
 2	Immunity	EN55024
 3	Electrical Safety	EN60950 (TUV), UL1950 (UL/cUL)

#### **Safety**



-  4  Power to the access point must be sourced only from the adapter.



#### **Europe—EC**



Use TÜV licensed AC adapter of 5 V DC, min 2.0 A.



#### **Other Countries**



Use a Safety Agency Approved AC adapter of 5 V DC, min 2.0 A.

-  5  **Caution:** Power cord is used as a disconnection device. To de-energise equipment disconnect the power cord.


-  6  **Lightning Danger**  
**Danger:** Do not work on equipment or cables during periods of lightning activity.

-  7  Do not block air vents.



-  8  **Operating Temperature:** This product is designed for a maximum ambient temperature of 65 degrees C.

-  9  **All Countries:** Install product in accordance with local and National Electrical Codes.

**Normen:** Dieses Produkt erfüllt die Anforderungen der nachfolgenden Normen.



- |   |          |                        |                                |
|---|----------|------------------------|--------------------------------|
|  | <b>1</b> | Hochfrequenzstörung    | EN55022 Klasse B               |
|  | <b>2</b> | Störsicherheit         | EN55024                        |
|  | <b>3</b> | Elektrische Sicherheit | EN60950 (TUV), UL1950 (UL/cUL) |



**Sicherheit**



-  **4**  Der Buchse darf nur aus dem Adapter Strom zugeführt werden.



**Europe—EC**



Gebrauchen Sie einen von TÜV zugelassenen Wechselstromadapter für Gleichstrom 5 Vdc, 2.0 A.

-  **5**  **Vorsicht:** Das netzkabel dient zum trennen der stromversorgung. Zur trennung vom netz, kabel aus der steckdose ziehen.

-  **6**  **Gefahr Durch Blitzschlag**  
**Gefahr:** Keine Arbeiten am Gerät oder an den Kabeln während eines Gewitters ausführen.

-  **7**  Entlüftungsöffnungen nicht versperren.

-  **8**  **Betriebstemperatur:** Dieses Produkt wurde für den Betrieb in einer Umgebungstemperatur von nicht mehr als 65° C entworfen.


-  **9**  **Alle Länder:** Installation muß örtlichen und nationalen elektrischen Vorschriften entsprechen.



**Standarder:** Dette produkt tilfredsstiller de følgende standarder.


- |   |                                     |                                |
|---|-------------------------------------|--------------------------------|
| 1 | Radiofrekvens forstyrrelsesemission | EN55022 Klasse B               |
| 2 | Immunitet                           | EN55024                        |
| 3 | Elektrisk sikkerhed                 | EN60950 (TUV), UL1950 (UL/cUL) |


**Sikkerhed**


- 4  Strømforsyningen til apparatet må udelukkende tages fra tilpasningstransformatoren.


**Europe - EC**


Brug kun TÜV godkendt vekselstrømstransformator på 5 Vdc, 2.0 A.

- 5  **Advarsel:** Den strømførende ledning bruges til at afbryde strømmen. Skal strømmen til apparatet afbrydes, tages ledningen ud af stikket.

- 6  **Fare Under Uvejr**  
**Fare:** UNDLAD at arbejde på udstyr eller KABLER i perioder med LYNAKTIVITET.

- 7  Ventilationsåbningerne må ikke blokeres.



- 8  **Betjeningstemperatur:** Dette apparat er konstrueret til en omgivende temperatur på maksimum 65 grader C.

- 9  **Alle Lande:** Installation af produktet skal ske i overensstemmelse med lokal og national lovgivning for elektriske installationer.

**Eisen:** Dit product voldoet aan de volgende eisen.



	<b>1</b>	RFI Emissie	EN55022 Klasse B
	<b>2</b>	Immunititeit	EN55024
	<b>3</b>	Electrische Veiligheid	EN60950 (TUV), UL1950 (UL/cUL)

### **Veiligheid**



-  **4**  Stroom mag alleen via de adapter naar het apparaat toegevoerd worden.



### **Europe - EC**


Gebruik een door TÜV gekeurde wisselstroomadapter van 5 Vdc, 2.0 A.

-  **5**  **Waarschuwing:** Het toestel wordt uitgeschakeld door de stroomkabel te ontkoppelen. Om het toestel stroomloos te maken: de stroomkabel ontkoppelen.

-  **6**  **Gevaar Voor Blikseminslag**  
**Gevaar:** NIET aan toestellen of KABELS WERKEN bij BLIKSEM.

-  **7**  Ventilatiegaten niet blokkeren.



-  **8**  **Bedrijfstemperatuur:** De omgevingstemperatuur voor dit produkt mag niet meer bedragen dan 65 graden Celsius.

-  **9**  **Alle Landen:** het toestel installeren overeenkomstig de lokale en nationale elektrische voorschriften.

**Normes:** ce produit est conforme aux normes de suivantes.



- |   |          |   |                                |
|---|----------|---|--------------------------------|
|  | <b>1</b> | Emission d'interférences radioélectriques | EN55022 Classe B               |
|  | <b>2</b> | Immunité                                  | EN55024                        |
|  | <b>3</b> | Sécurité électrique                       | EN60950 (TUV), UL1950 (UL/cUL) |



#### **Sécurité**



-  **4**  L'alimentation du concentrateur doit être uniquement fournie par l'adaptateur.



#### **Europe - EC**



Utiliser un adaptateur secteur conforme TÜV de 5 V dc, 2.0 A en courant continu.

-  **5**  **Attention:** Le cordon d'alimentation sert de mise hors circuit. Pour couper l'alimentation du matériel, débrancher le cordon.
















-  **6**  **Danger De Foudre**  
**Danger:** NE PAS MANIER le matériel ou les CÂBLES lors d'activité orageuse.

-  **7**  Ne pas bloquer les fentes d'aération.







-  **8**  **Température De Fonctionnement:** Ce matériel est capable de tolérer une température ambiante maximum de 65 degrés Celsius.

-  **9**  **Pour Tous Pays:** Installer le matériel conformément aux normes électriques nationales et locales.

**Standardit:** Tämä tuote on seuraavien standardien mukainen.

- |   |          |                        |                                |
|---|----------|------------------------|--------------------------------|
|  | <b>1</b> | Radioaaltojen häirintä | EN55022 Luokka B               |
|  | <b>2</b> | Kestävyys              | EN55024                        |
|  | <b>3</b> | Sähköturvallisuus      | EN60950 (TUV), UL1950 (UL/cUL) |
- Turvallisuus
-  **4**  Tähtipisteeseen (hub) syötettävän virran pitää tulla ainoastaan sovittimesta.
- Europe - EC**  
Käytä TÜV-lisenssillä valmistettua verkkosovitinta, jonka tasajännitteen nimellisarvot ovat 5 Vdc, 2.0 A (milliampeeria).
-  **5**  **Huomautus:** Virtajohtoa käytetään virrankatkaisulaitteena. Virta katkaistaan irrottamalla virtajohto.
-  **6**  **Salamaniskuvaara**  
**Hengenvaara:** ÄLÄ TYÖSKENTELE laitteiden tai KAAPELEIDEN KANSSA SALAMOINNIN AIKANA.
-  **7**  Älä tuki ilmareikiä
-  **8**  **Käyttölämpötila:** Tämä tuote on suunniteltu ympäröivän ilman maksimilämpötilalle 65° C.
-  **9**  **Kaikki Maat:** Asenna tuote paikallisten ja kansallisten sähköturvallisuusmääräysten mukaisesti.


**Standard:** Questo prodotto è conforme ai seguenti standard.

- |   |  |                                |
|---|--|--------------------------------|
| 1 | Emissione RFI (interferenza di radiofrequenza) | EN55022 Classe B               |
| 2 | Immunità                                       | EN55024                        |
| 3 | Sicurezza elettrica                            | EN60950 (TUV), UL1950 (UL/cUL) |
- Norme Di Sicurezza
- 4  Questo dispositivo deve essere alimentato solo mediante l'adattatore.
- Europe - EC**  
Utilizzare l'adattatore per c.a. da 5 Vdc, 2.0 A conforme alla normativa TÜV.
- 5  **Attenzione:** Il cavo di alimentazione è usato come dispositivo di disattivazione. Per togliere la corrente al dispositivo staccare il cavo di alimentazione.
- 6  **Pericolo Di Fulmini**  
**Pericolo:** NON LAVORARE sul dispositivo o sui CAVI durante PRECIPITAZIONI TEMPORALESCE.
- 7  Non ostruire le prese d'aria.
- 8  **Temperatura Di Funzionamento:** Questo prodotto è concepito per una temperatura ambientale massima di 65 gradi centigradi.
- 9  **Tutti I Paesi:** installare il prodotto in conformità delle vigenti normative elettriche nazionali.

**Sikkerhetsnormer:** Dette produktet tilfredsstiller følgende sikkerhetsnormer.


- |   |                     |                                |
|---|---------------------|--------------------------------|
| 1 | RFI stråling        | EN55022 Klasse B               |
| 2 | Immunitet           | EN55024                        |
| 3 | Elektrisk sikkerhet | EN60950 (TUV), UL1950 (UL/cUL) |


**Sikkerhet**


- 4  All strømtilførsel må komme fra adapteren.


**Europe - EC**


Benytt TÜV-godkjent AC-adapter på 5 Vdc, 2.0 A (milliampere).

- 5  **Forsiktig:** Strømledningen brukes til å frakoble utstyret. For å deaktivisere utstyret, må strømforsyningen kobles fra.

- 6  **Fare For Lynnedslag**  
**Fare:** ARBEID IKKE på utstyr eller KABLER i TORDENVÆR.

- 7  Blokker ikke luftventilene.


- 8  **Driftstemperatur:** Dette produktet er konstruert for bruk i maksimum romtemperatur på 65 grader celsius.

- 9  **Alle Land:** Produktet må installeres i samsvar med de lokale og nasjonale elektriske koder.

**Padrões:** Este produto atende aos seguintes padrões.


- |     |   |                                |
|-----|---|--------------------------------|
| ✍ 1 | Emissão de interferência de radiofrequência | EN55022 Classe B               |
| ✍ 2 | Imunidade                                   | EN55024                        |
| ✍ 3 | Segurança eléctrica                         | EN60950 (TUV), UL1950 (UL/cUL) |


#### **Segurança**


- ✍ 4  Use somente o adaptador fornecido para alimentação elétrica do hub.


#### **Europe - EC**


Use um adaptador de corrente alternada com saída DC de 5 Vdc, 2.0 A em conformidade com as especificações da TÜV.

- ✍ 5  **Cuidado:** O cabo de alimentação é utilizado como um dispositivo de desconexão. Para deseletrificar o equipamento, desconecte o cabo de ALIMENTAÇÃO.

- ✍ 6  **Perigo De Choque Causado Por Raio**  
**Perigo:** NÃO TRABALHE no equipamento ou nos CABOS durante períodos suscetíveis a QUEDAS DE RAIOS.

- ✍ 7  Não bloqueie as aberturas de ventilação.



- ✍ 8  **Temperatura De Funcionamento:** Este produto foi projetado para uma temperatura ambiente máxima de 65 graus centígrados.

- ✍ 9  **Todos Os Países:** Instale o produto de acordo com as normas nacionais e locais para instalações elétricas.

**Estándares:** Este producto cumple con los siguientes estándares.



	<b>1</b>	Emisión RFI	EN55022 Clase B
	<b>2</b>	Inmunidad	EN55024
	<b>3</b>	Seguridad eléctrica	EN60950 (TUV), UL1950 (UL/cUL)

### **Seguridad**



-  **4**  La energía para el dispositivo central o “hub” debe provenir únicamente del adaptador.



### **Europe - EC**



Utilizar un adaptador de corriente alterna autorizado TÜV de 5 Vdc, 2.0 A.

-  **5**  **Atencion:** El cable de alimentacion se usa como un dispositivo de desconexion. Para desactivar el equipo, desconecte el cable de alimentación.

-  **6**  **Peligro De Rayos**  
**Peligro:** NO REALICE NINGUN TIPO DE TRABAJO O CONEXION en los equipos o en LOS CABLES durante TORMENTAS ELECTRICAS.

-  **7**  No bloquee las aberturas para ventilacion.

-  **8**  **Temperatura Requerida Para La Operación:** Este producto está diseñado para una temperatura ambiental máxima de 65 grados C.



-  **9**  **Para Todos Los Países:** Monte el producto de acuerdo con los Códigos Eléctricos locales y nacionales.



**Standarder:** Denna produkt uppfyller följande standarder.



	<b>1</b>	Radiostörning	EN55022 Klass B
	<b>2</b>	Immunitet	EN55024
	<b>3</b>	Elsäkerhet	EN60950 (TUV), UL1950 (UL/cUL)



#### **Säkerhet**



-  **4**  Endast anslutningsenheten får vara kraftkälla till centralen.



#### **Europe - EC**



Använd en växelströmsanslutningsenhet licensierad av TÜV. Likström 5 Vdc, 2.0 A.

-  **5**  **Varning:** Nätkabeln används som strömbrytare för att koppla från strömmen, dra ur nätkabeln.

-  **6**  **Fara För Blixtnedslag**  
**Fara:** ARBETA EJ på utrustningen eller kablarna vid ÅSKVÄDER.

-  **7**  Blockera inte luftventilerna.

-  **8**  **Driftstemperatur:** Denna produkt är konstruerad för rumstemperatur ej överstigande 65 grader Celsius.

-  **9**  **Alla Länder:** Installera produkten i enlighet med lokala och statliga bestämmelser för elektrisk utrustning.

# Glossary

---

## **ARP (Address Resolution Protocol)**

The protocol used by TCP/IP networks to relate IP addresses with the physical network addresses of network interfaces.

## **BFSK (Binary Frequency Shift Key)**

A broadcasting method that lengthens the range but halves the throughput as compared to the QFSK method.

## **bridge**

A device that expands a local area network by forwarding frames between data link layers associated with two separate physical media types, usually carrying a common protocol. A bridge connects wireless devices to a wired network and allows connection of networks or subnetworks with similar architectures.

## **broadcast**

A type of transmission in which a message sent from the host is received by many devices on the system.

## **channel**

The path for transmitting data from a device to the host computer. A port may contain one or more logical channels. In 2.4 GHz RF networks, the channel refers to the frequency hopping sequence the radio follows.

**data link tunneling**

An access point encapsulates an Ethernet frame in a data frame and forwards the frame to the next access point on the path to the final destination. Data link tunneling is used to make mobility transparent to the underlying network or to isolate the radio traffic from terminals on an Ethernet segment. Data link tunneling occurs automatically when Ethernet bridging is disabled on the root access point. Ethernet bridging is automatically disabled on a secondary LAN if there is no designated bridge for the secondary LAN. An access point that has Ethernet bridging disabled forwards a frame inbound on its Ethernet port using data link tunneling. The root access point or a designated bridge for a secondary LAN uses data link tunneling to forward frames outbound to access points on the same Ethernet segment.

**designated bridge**

An access point that is assigned the role of bridging frames destined for or received from a secondary LAN. A designated bridge, or secondary LAN bridge, connects a secondary LAN with the primary LAN. In the access point, the secondary LAN bridge priority parameter determines if the access point is a candidate to become the designated bridge.

**DHCP (Dynamic Host Configuration Protocol)**

An Internet standard stack protocol that allows dynamic distribution of IP address and other configuration information to IP hosts on a network. Implementation of the DHCP client in Allied Telesyn network devices simplifies installation because the devices automatically receive IP addresses from a DHCP server on the network.

**distribution LAN**

Any Ethernet LAN attached to access points that are bridging between the Ethernet LAN and the radio network. At any given time, only one access point in a distribution LAN provides access to the Ethernet LAN for a given node in the domain.

**DIX**

A standardized Ethernet frame format developed by Digital Equipment Corporation, Intel Corporation, and Xerox. Another frame format is 802.3.

**flooding**

A frame is flooded when the destination location is unknown. The destination location of a multicast frame is never known. Unicast and multicast flooding parameters determine how a flooded frame is forwarded.

**home IP subnet**

The IP subnet that contains the wired primary LAN and any wireless extensions of the subnet.

**IGMP (Internet Group Management Protocol)**

IGMP is a protocol that allows the access point to have more than eight IP tunnels. IGMP allows an access point to participate in an IP multicast group without any special router configuration.

**inbound frames**

Frames moving toward the primary LAN.

**IP subnet**

A single member of the collection of hardware networks that composes an IP network. Host addresses on a given subnet share an IP network number with hosts on all other subnets of the IP network. The local address is divided into subnet-number and host-number fields to indicate which subnet a host is on.

**MAC address**

There are 2 types of MAC addresses: unicast and broadcast. Unicast specifies a single Ethernet interface, while multicast specifies a group of Ethernet addresses. Broadcast is a variation of multicast in which a multicast is received by all interfaces.

**MIB (Management Information Base)**

This repository stores network traffic information that SNMP management programs collect. Your network administrator can use management software interacting with the MIB to obtain information about network activity. Contact your local Allied Telesyn representative to learn how to obtain a copy of the MIB for the access point.

**multicast address**

A form of broadcast address through which copies of the frame are delivered to a subset of all possible destinations that have a common multicast address.

**non-bridging secondary LAN**

A secondary LAN that does not have a designated bridge. A non-bridging secondary LAN is used to connect access points without using wireless hops.

**outbound frames**

Frames moving away from the primary LAN.

**peer-to-peer network**

A type of LAN whose workstations are capable of being both clients and servers.

**point-to-point bridge**

A wireless link that connects two wired Ethernet segments. Two access points can be used to provide a point-to-point bridge between two buildings so that wired and wireless devices in each building can communicate with devices in the other building.

**primary bridging**

Ethernet bridging on a root port. An access point uses primary bridging to bridge frames to and from the Ethernet network on its root port. Note that primary bridging is not the same as bridging to the primary LAN.

**primary LAN**

The Ethernet LAN attached to the access point that is acting as the root. The primary LAN is typically the LAN on which the servers are located. Primary and secondary LANs are both distribution LANs.

**QFSK (Quad Frequency Shift Key)**

A broadcasting method that shortens the range but doubles the throughput as compared to the BFSK method.

**remote subnet**

An Ethernet segment other than the primary LAN. A remote subnet is a secondary LAN.

**remote IP subnet**

A secondary LAN attached to the network through an IP tunnel.

**root**

The access point with the highest root priority becomes the root of the network spanning tree. If the root becomes inactive, the remaining root candidates negotiate to determine which access point becomes the new root. The root can be used to set system-wide flooding and RF parameters. The root is also the only node in the network that can originate IP tunnels.

**root port**

The access point port that provides the inbound connection to the spanning tree. The root port provides a link to a parent access point. Note that a root access point does not have a root port.

**root subnet**

The Ethernet segment to which the root access point connects, also known as the primary LAN.

**router**

A software and hardware connection between two or more subnetworks that permits traffic to be routed from one network to another on the basis of the intended destinations.

**secondary bridging**

Ethernet bridging on a non-root port. An access point that is the designated bridge for a secondary LAN uses secondary bridging to bridge frames to and from the secondary LAN on a non-root Ethernet port.

**secondary LAN**

Any Ethernet LAN that is not the primary LAN. A single access point functions as the designated bridge for a secondary LAN. The designated bridge attaches the secondary LAN to the network through a radio link or an IP link. Primary and secondary LANs are both distribution LANs.

**SNAP**

A protocol extension typically used by Appletalk networks.

**SNMP (Simple Network Management Protocol)**

SNMP is a popular network management protocol in the TCP/IP and SPX/IPX protocol suite. SNMP allows TCP/IP and SPX/IPX sites to exchange configuration and status information. It uses management programs called "agents" to monitor network traffic. SNMP stores the information it collects in the Management Information Base (MIB). Your network administrator can use management software interacting with the MIB to obtain information about network activity.

**spanning tree**

A form of network organization in which each device on the network has only one path to the root. The access points automatically configure into a self-organized network that provides efficient, loop-free forwarding of frames through the network.

**subnet**

A single member of the collection of hardware networks that compose an IP network. Host addresses on a given subnet share an IP network number with hosts on all other subnets of that IP network.

**triangular routing**

The routing logic used for a mobile IP end device that has roamed to a foreign network. Frames destined for a mobile end device are always sent to the home subnet of the end device. If the end device has roamed to another subnet, the frame must be forwarded to the remote subnet where the end device currently resides.

**access point**

The access point bridges frames between a wired Ethernet network and a wireless RF network. The access point can also serve as a bridge between two RF networks. The AT-WL2411 features Radio Independent and Network Independent architecture.

**unicast address**

A unique Ethernet address assigned to a single device on the network.

**WAP**

A wireless network device that serves as a repeater. It transmits data between an access point that is connected to the Ethernet network and end devices.

## **WEP**

Wired Equivalent Privacy, a feature that can be enabled in the IEEE 802.11b HR radio that allows data encryption for wireless communications.

## **wireless bridging**

A wireless link that connects two wired Ethernet segments. Two access points can be used to provide a point-to-point or wireless bridge between two buildings, so that wired and wireless devices in each building can communicate with devices in the other building.